CLOUD COMPUTING AND ITS SECURITY ASPECTS

Subhash Basishtha[1], Saptarshi Boruah[2]

[1]*Department of Information Technology, Assam University, Silchar-788011, India*
[2]*Department of Information Technology, Assam University, Silchar-788011, India*

Abstract

Cloud computing is a new computing paradigm in the field of it that provides hosted services to a large number of user on demand basis over the internet. They are internet based network that has large numbers of servers. It allows to use the services only when you want and pay only for the amount what you have used. Since cloud computing share distributed resources over an open environment, so security becomes a major concern here. To improve the work performance different services are distributed on different servers but the security and safety aspects are remaining insufficient. Security is the one of major issues that hampers the growth of cloud. So, in this paper we first try to give an idea about cloud computing and then concentrate on the major security aspects of cloud computing paradigm.

Keywords: *Cloud Computing, IT, Infrastructure, cloud, Security.*

----------***----------

1. INTRODUCTION

Cloud computing is the latest trend in the IT field. It is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. This technology has the capacity of allocating resources to its user on request over the network. In cloud computing we can obtain networked storage space and computer resources. With the help of cloud it is possible to access the information from anywhere at any time. The cloud removes the need of to be in the same physical location as the hardware. The cloud provider both own and house the hardware and software necessary to run your application. It is mainly developed to cut the operational and capital costs so that IT department can focus on strategic projects instead of keeping the datacenter running. In the last few years cloud computing becomes one of the fast growing technology in the IT industry. As more and more information of individual or companies are placed on the cloud, security becomes a major concern. Security issues play a significant role in slowing down its acceptance.

One way of thinking cloud computing is to consider the experience with email. In case of email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support client personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important requirement is having internet access. Your email is not housed on your physical computer; you access it through an internet connection, and you can access it anywhere. An email client is similar to how cloud computing works. Except instead of accessing just your email, you can choose what information you have access to within the cloud. [3]

2. SURVEY ON CLOUD SECURITY

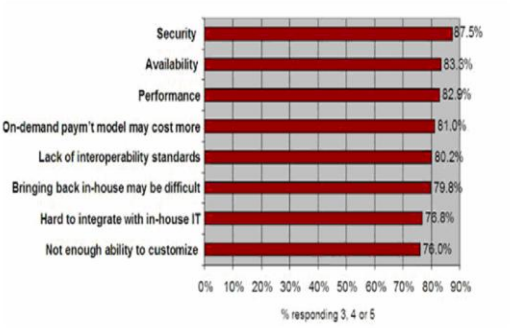

Fig 1: Ranking of security in cloud computing as surveyed by IDC. [5]

The Fig: 1 shows the survey on security. This represents security as first rank according to IT executives. This information is collected from 263 IT professional by asking different question related to the cloud, and many of the executives are worried about security perspective of cloud. [5]

3. OVERVIEW

The cloud is helpful for the businesses or companies that cannot afford the hardware or the storage space that they required. With the help of cloud they can store their information in the cloud and can the use the computer resources. Thus removing the cost of purchasing the memory devices and other hardware. They only have to pay the amount for the uses of the space over cloud and for the other services as well. Your company need not to pay for hardware and maintenance; the service provider will pay for hardware and maintenance.

That is, use as much or as less you need, use only when you want, and pay only what you uses.

The only requirement to use the cloud is that to access the cloud you must have an internet connection.

The term Cloud Computing was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams.

Key benefits of cloud computing: [6]

- Flexibility – There is the ability to update hardware and software quickly based on customer demands and updates in technology.
- Savings – There is a reduction of capital expenditures and IT personnel.
- Location & Hardware Independence – Users can access application from a web browser connected anywhere on the internet.
- Multi-tenancy – Resources and cost are shared among many users, allowing overall cost reduction.
- Reliability – Many cloud providers replicate their server environments in multiply data centers around the globe, which accounts for business continuity and disaster recovery.
- Security – Centralization of sensitive data improves security by removing data from the users' computers. Cloud providers also have the staff resources to maintain all the latest security features to help protect data.
- Maintenance – Centralized applications are much easier to maintain than their distributed counterparts. All updates and changes are made in one centralized server instead of on each user's computer.

4. CLOUD COMPONENTS

In simple, cloud computing is made up of several components: the clients, the data centers and the distributed servers. Each element has a specific role in delivering a functional cloud based application.[14]

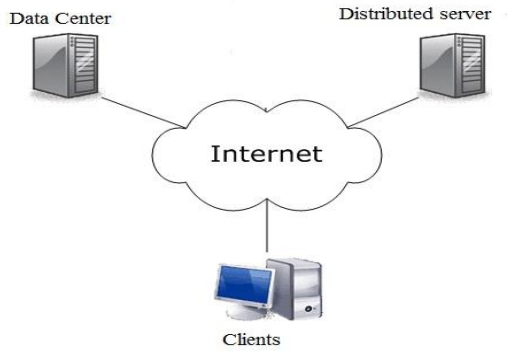

Fig 2: Cloud Components

4.1 Clients

The clients are the devices that the end users interact with to manage their information on the cloud. They are generally categorized into three types:

a) Mobile: mobile devices include PDA or Smartphone.
b) Thin: thin clients are computers that don't have internal hard drives rather server do the entire task and then only display the information.
c) Thick: thick clients are the regular computer that use web browser like Firefox or internet explorer to connect to the cloud.

Among them thin clients are becoming popular because of the reason as mentioned below:

- Thin clients are cheaper because they don't contain much hardware.
- Thin clients are managed at the server so there is less chance of failure.
- Since all the processing is done by server and there is no hard drive therefore there is less number of security problems.
- Since all the data are stored on the server so there is less chance of lost of data if client computer is crashed or stolen.

4.2 Data Centre

Datacenter is the collection of servers where the applications are hosted so that clients can use them to operate on their business. The software and the data are stored on the server. This structure reduces capital expenditures, since the business only pays for the resources that they have used.

4.3 Distributed Server

In cloud computing the servers are not kept at the same location they are distributed geographically at different location. This gives the service providers more flexibility in options and security. For instance in case of Amazon, their cloud is distributed in server all over the world. If something is happen to one site then it could be accessed through another site also.

5. TYPES OF CLOUD

There are different types of clouds that you can subscribe depending on your needs. As a home user or small business owner, you will most likely use public cloud services.

a) Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space. [3] It is typically based on a pay-per-use model. 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. [8]

b) Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.[3] 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.

c) Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community. [3]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. [4]

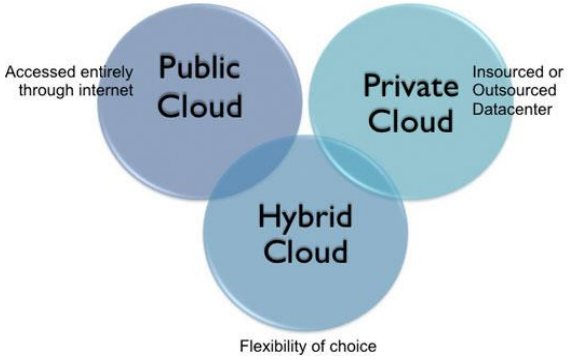

Fig3: Cloud Computing Types

5.1 Choosing the Cloud Providers

Each provider serves a specific function, giving users more or less control over their cloud depending on the type. When you choose a provider, compare your needs to the cloud services available. Your cloud needs will vary depending on how you intend to use the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if you will be using the cloud for business. Keep in mind that your cloud provider will be pay-as-you-go, meaning that if your technological needs change at any point you can purchase more storage space (or less for that matter) from your cloud provider. [3]

There are three types of cloud providers that you can subscribe to. They are: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). [15]

a) **SaaS:** A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.

b) **PaaS:** A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.

c) **IaaS:** An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.

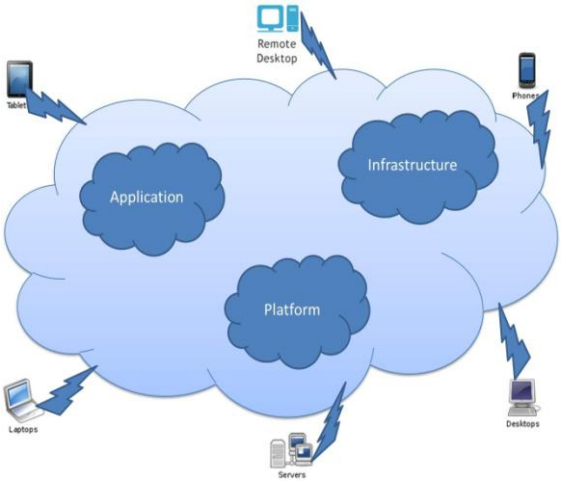

Fig 4: Cloud computing Architecture [13]

SaaS, e.g., Google Docs [10]
PaaS, e.g., Google AppEngine [11]
IaaS, e.g., Amazon EC2 [12]

6. SECURITY ASPECTS

Security plays the major role in cloud computing acceptance. There is a lot of personal information and potentially secure data that people store in the personal computers. When this information is transferred to cloud then there should be precautions to secure the data. Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks. Some of security issues are as follows: [1]

a) Confidentiality:

- There is always a fear whether the sensitive data remain confidential after transferring it to the cloud.
- Will the cloud providers be honest and will not peek the data.

b) Integrity:

- How the clients will know that cloud provider is doing the computations correctly.

- How the clients know that data are preserved without tampering it.

c) Availability:

- What happens if the cloud providers go out of business?
- What happens if cloud providers are attacked in a denial of service attack?

d) Privacy issues:

- Cloud stores data from a large number of clients so privacy becomes a major concern.

e) Additional attacks:

- Entity outside the organisation can store and compute data so attackers can easily target the communication link between the cloud providers and the client.

For resolving some cloud security issues we need to adapt well known techniques and should perform new research and innovate to make clouds secure.

6.1 Security Issues in SaaS

Following key security element should be carefully considered as an Integral part of the SaaS deployment process: [2]

a) Data Security
b) Network Security
c) Data locality
d) Data integrity
e) Data access
f) Data Segregation
g) Authorization and Authentication
h) Data Confidentiality
i) web Application security
j) Availability
k) Backup

6.2 Security Issues in PaaS

- In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider.
- Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security (Oracle, 2009).The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the electiveness of the application security programs.
- Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.[2]

6.3 Security Issues in IaaS

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defence as the main method to protect their datacenter. It may also revoke compliance and breach security policies. OS Security issues also alive in IaaS. Following are the points which are considered in IaaS.

Security Attacks in Cloud:

- Denial of Service (DoS) attacks: Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging.
- Side Channel attacks: An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.
- Authentication attacks: Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.
- Man-in-the-middle cryptographic attacks: This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.
- Network Security:
  a) Network penetration and packet analysis.
  b) Session management weaknesses
  c) Insecure SSL trust configuration.[2]

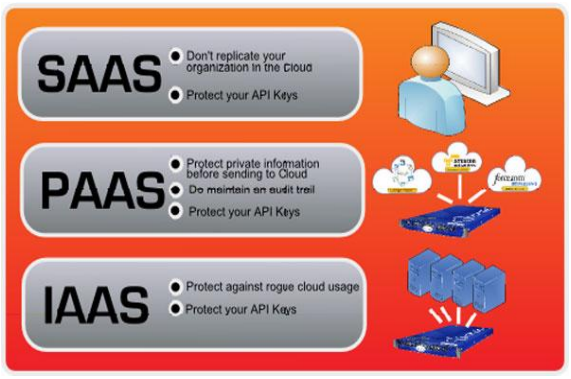

Fig 5: Security issues in Cloud Models [10]

7. CONCLUSIONS

The cloud providers give many options to its users by increasing the ease of access to its resources by simply connecting to the internet. However this ease of use is also come up with drawbacks as you have less control over your data and have little knowledge of where the data is kept. You must be aware of the security risks of having data stored on the cloud as the cloud is a big target for the attackers and it is having the disadvantage that it can be accessed through an unsecure internet connection.

Before starting with the cloud computing we should clearly understand that what type of cloud will be best for our needs, what type of provider will be most useful to our etc?

FUTURE WORK

Cloud computing has the potential to become a secure and economically viable IT solution in future. We need much more technical and non-technical solution to make the technology work and become more secure in practical. This paper only represents the basic concepts and some of security aspects of cloud computing. We need more modification here. So, in future we want to do more work on the security field of the cloud computing paradigm.

ACKNOWLEDGEMENTS

We the authors are very graceful to our respected sir Ajoy Kumar Khan of Assam University Silchar for inspiring and guide us to complete this paper successfully and the department of IT, Assam University for providing us such an environment.

REFERENCES

[1] Ragib Hasan," Security and Privacy in Cloud Computing", Johns Hopkins University, en.600.412 Spring 2010.

[2] Amar Gondaliya," Security in Cloud Computing", Hasmukh Goswami College of Engineering, Ahmedabad.

[3] Alexa Huth and James Cebula," The Basics of Cloud Computing", US-CERT.

[4] Kuyoro S. O., Ibikunle F. & Awodele O. ,"Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[5] F. A. Alvi1, Ψ, B.S Choudary2, N. Jaferry3, E.Pathan4, "A review on cloud computing security issues & challanges".

[6] Paul Stryer, "Understanding Data Centers and Cloud Computing", Global Knowledge Training LLC.

[7] Article on Security Considerations for Platform as a Service (PaaS) http://social.technet.microsoft.com/wiki/contenco/articles/3809.security-considerations-for-platform-as-a-service-paas.aspx

[8] Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service" International Journal of Advanced Research in Computer Science and Software Engineering.

[9] Article on SaaS, PaaS, and IaaS: A security checklist for cloud models http://www.csoonline.com/article/660065/saas-paas-and-iaas-a-security-checklist-for-cloud-models

[10] Introduction to Google Docks http://en.wikipedia.org/wiki/Google_Docs

[11] Charles Cheverance, "Google Application Engine Introduction", University of Mitchigan.

[12] Mike culver, Melody Ng, Jeson Chan "Introduction to Amazon EC2 running IBM", Amazon web services.

[13] Cloud Computing and types of cloud http://cloudblog.8kmiles.com/2012/02/27/cloud-computing-type/

[14] Barrie Sosinsky "Cloud Computing Bible", Wiley India Pvt Ltd (2011),ISBN-13-9788126529803,2nd edition

[15] George Reese "Cloud Application Architectures 1st Edition", Shroff/o'reilly (2009), ISBN-13 9788184047141, 1stEdition.