

Cloud computing: A brief descriptive review along with its security issues and challenges

Akansha Singh

Dept. of Computer Science and Engineering, Goel Institute of Technology and Management
Dr. APJ Abdul Kalam University
Lucknow, India

Abstract: The present era is accepting and utilizing the latest technologies rapidly. The emergence of cloud technology is rapidly being utilized by organizations as cloud provides them to have maximum resources for rapid development with investment of minimal cost.

There exist many papers and review papers on cloud and almost everyone is individually capable of clarifying the technical aspect of the technology. Like any other technology cloud also have several aspects and vision of study, each phase is crucial to understand and so is with cloud computing. All the previous papers being written have some aspects missing in between these different theories.

This paper basically focuses on the description of cloud computing technology, its features and architectural models along with the security issues and design principles kept in mind before implementing cloud in entirely different way. The paper is modeled in three parts: (1) The theoretical description of cloud, (2) architectural models of cloud, (3) security issues and challenges faced in the implementation of cloud.

It is specially suggested as suitable for beginners pursuing their research in cloud security domain to find the basic research problems regarding security and issues found in cloud security.

Keywords: Cloud computing, cloud security, IaaS, PaaS, SaaS.

I. INTRODUCTION

In the past few years as the pace of development is increased in each and every field. The amount of data is also increased along with the requirement of resources to generate and store the data. Organizations are growing and also their requirements, thus making it practically impossible to have all the resource and use them completely to insure maximum resource utilization in minimum cost. Computing on desktop is not capable of providing maximum resources and sharing of data at global level is also not convenient, so to computing on desktop can be replaced by computing on internet.[7]

Informally we can state that cloud is basically computing of data on internet rather computing and processing the data on desktop. Cloud provides a platform for processing and storing data on internet which intern provides various other benefits like:

1. Cost saving: cloud computing provides a cost efficient mechanism for handling and controlling the overall data being consumed and generated by any organization .It

is easy and cost efficient to rent the resources rather purchasing them.

2. Pay-as-you-go service: this service is one of the most important reasons why cloud is so popular. The organizations can rent and pay for only those services and infrastructure they are using from the cloud service providers. All the other services that are not required or used by the organization can be discarded easily.
3. Security from internal agents: The threat to the data is not only by external agents but also by internal agents and employees. So cloud computing provides a mechanism to insure security from internal agents as well as external security threats.
4. Flexibility: Any organization can easily add on new infrastructure or service and also remove whenever required. Cloud computing is highly flexible in terms of renting the resources and discarding them from time to time.
5. Mobility: For an organization where the salesmen are mostly travelling and need to access the data remotely, Cloud is the best way out. As cloud provides easy access to data from any source to any destination like phones, laptops etc.
6. Insight: For an IT company the data is equivalent to money. All the IT companies and organizations are very specific to their data and its security for future utilization, planning and decision making. Cloud provides a mechanism to summarize the crucial data which intern helps for easy, less time consuming decision making.
7. Disaster recovery: As the data in cloud in not physically present in actual desktop or device using cloud but the data is stored in abstract format at distinct location. Since the infrastructure is not physically located nearby geographical region at one place hence the data is assumed to be safe from natural disasters.
8. Automatic software update: Updating of the cloud software and other modifications are not organizations responsibility rather it is the responsibility of the service provider to provide updations time to time.
9. Sustainability: Cloud infrastructure is an economically state and environmentally sustainable development.

It is easy to tenant the resources and infrastructure rather to physically purchase them, by this one organization can use maximum resources in minimum cost and can utilize this capital in other places of requirement.[1]

According to NIST (national institute of standards and technology) , " cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources(e.g. network , serves , storage, application and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [8]

A. Features of Cloud Computing:

Cloud computing provides us many special features which draw the attention of all the business sector, organizations and industries. Some basic features of cloud computing according to NIST (national institute of standards and technology) are as follows:

1. On demand self-service: A consumer with all the appropriate rights can easily ask for computing capabilities without any human interactions like CPU time, storage, network, server time, etc.
2. Broad network access: A customer can purchase the cloud through any medium by the access can be made broadly by any other device like mobiles, laptops, desktops etc.
3. Resource pooling: Pooling of resources can be easily done by multiple customers using a multi-tenant model.
4. Elasticity: Cloud provides capabilities to increase and decrease the no of resources rented by the customer at any instance of time.
5. Measured Services: Cloud systems automatically controls and optimizes resources being used by any consumer. The cloud itself keeps the track of all the records regarding the utilization of storage, processing, bandwidth, user's accounts etc.

B. Limitations Of Cloud Computing

All the new technologies being introduced are always having some merits over the previously used mechanism at that place but there do exists some or the other downsides of the newly introduced concept. Taking cloud into consideration one must be very specific before choosing any service provider as any organization totally rely on the outsider and handles all the data to the outsider for processing and management.

The benefits and merits of cloud are immense but the idea to consider all the negative points before investment of time, money and data may develop down the road. [1]

1. Downtime & Dependability:

Since cloud is operated by internet itself and internet connection can be lost for some instance of time hence the overall working/production has to be paused unless and until the connection is resumed. This leads to the

inability of organization onto the internet. [3]

In the similar way, consider that the cloud service provider has all the data relevant and crucial to the organization and due to some reasons stops all the services being provided by the service provider. Also in this case, the organization tenanted by the cloud is totally dependent on the service provider for all its management.

2. Security and Privacy:

Security is one of the most important issues that need to be considered while purchasing the cloud. The access of data in the cloud is done by many members from same organization and also from external agents from any other organizations. Due to which security becomes one of the most important issue.

The concept of cloud was coined with the assumption of security and ease to access go hand in hand but as the utilization of cloud has increased the security threats have also increased and the data security of any organization its always in priority. So the term private cloud was coined into existence to solve this problem.

3. Vulnerability to attack:

Cloud is completely implemented and used on internet and hence it is most vulnerable to attacks from various external and internal agents. The best ways to secure the data from attacks are:

- Make security goals the primary concern.
- Keep all the team members up to date with all the security issues and solutions.
- Be updated about all the hacks and security threats by reading security blogs.
- Classify the data and apply access controls
- Rotate or regularly change the keys and passwords.

4. Limited control and flexibility:

The control is always limited in terms of access and management in cloud technology the dependency of organizations is mostly towards vendors and service providers. The modification can only be done at root levels by the vendors.

II. MODELS AND ARCHITECTURE OF CLOUD COMPUTING

A. A Layered Architecture of Cloud Computing

In general, cloud computing has four layers in its fundamental architecture: The hardware/datacenter layer, the infrastructure layer, the platform layer and the application layer, as shown in Fig. 1. Each layer is described as following: [4]

1. The hardware layer: This layer is responsible for managing all the hardware resources of any cloud like physical servers, routers, switches, power and cooling systems. [4]
2. The infrastructure layer: This layer is also referred as virtualization layer creates a virtual pool of computing

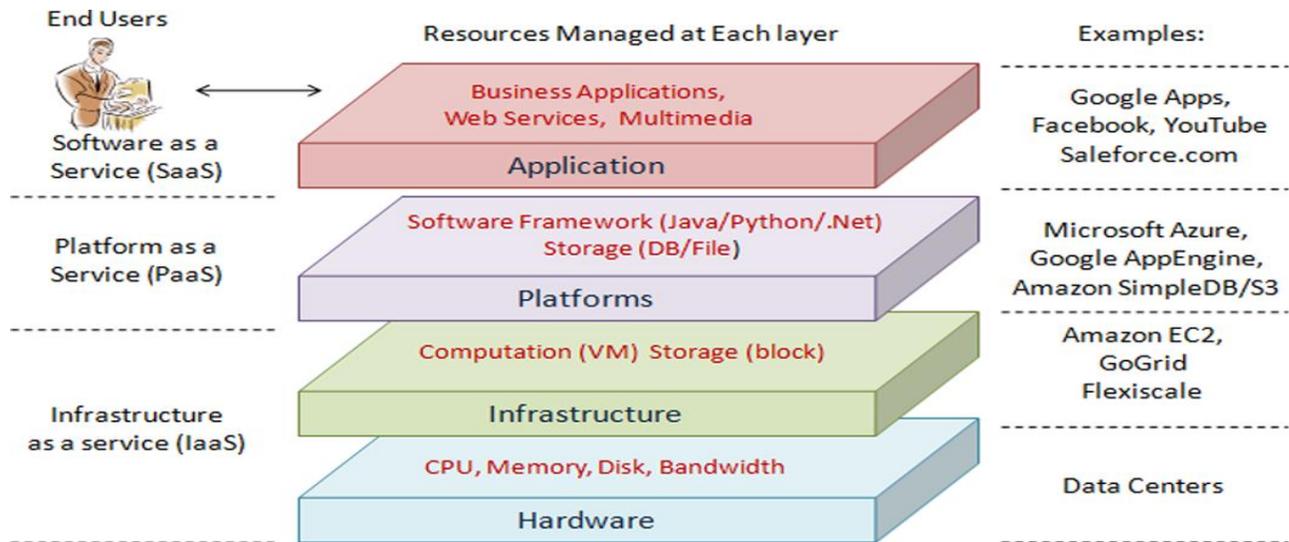


Fig. 1 Cloud computing architecture

Resources and storage space for distinguishing the cloud from physical resources. [6]

- The platform layer: Built upon the infrastructure layer, platform layer contains operating system and application framework to reduce the burden on deploying applications.[6]
- The application layer: The highest level of the hierarchy is the application layer containing the actual cloud application. Unlike traditional applications, cloud applications helps to achieve low operating cost and better availability and performance.[4]

B. Different Models Of Cloud

There are different types of cloud available; any organization can rent a cloud according to their own use and requirement:

1. **Public Clouds:** The clouds where the services like infrastructure, storage, resources etc. are provided off site on the internet are known as public clouds. [7]

Pros:

- These are least expensive clouds with no dedicated associated hardware and software.
- In such clouds, the cost is minimal as one has to pay for only those services that they are utilizing, also these have minimum maintenance cost.
- It provides large flexibility and scalability in terms of adding or removing any service at any instance of time.

Cons:

- Security of data is the major concern in such type of cloud as the whole data is present on internet.
- These clouds also face performance issues due to high traffic and latency over the network.

2. **Private Clouds:** The one where services are dedicated to any single organization and its registered members fall under this category. [7]

Pros:

- These are managed by private networks hence insuring greatest level of security.
- Performance is typically high due to dedicated hardware and software and networks with no latency.
- There is complete control of the organization over the entire set of hardware and software.

Cons:

- Higher cost due to dedicated infrastructure.
- Private clouds are growing very rapidly hence making IT and network latency.

3. **Hybrid Cloud:** These are the combination of private and public cloud technology as per the organizations requirement. The only limitation of this technology is that the customer has to keep track of multiple security platforms and ensure all the aspects of business can communicate with each other. [7]

Pros:

- It provides best of both the clouds- private & public i.e. security like private cloud and ease of data access like public clouds.

Cons:

- Storage, processing etc. is very difficult between public and private interface.
- It costs even more than a dedicated private cloud.

C. Architectural Models Of Cloud

- Infrastructure as a service (IaaS):** The customer here can buy and manage virtual infrastructure and utilize it as an actual personal

infrastructure like processing and storage. Authentication can be implemented through various means like what a person knows or has. And based on this authentication is provided to multiple users through these properties.

It is the easiest way of utilizing resources where the customer cannot touch the hardware but can use it virtually. Also cloud infrastructure is not limited to a single server but relies on pool of shared servers.

In this system the infrastructure is virtually connected over internet; where a trusted third party is charged with maintenance and allocation.

b. Platform as a service (Paas):

Cloud platform are offered as a service over internet with no need to install and update the or even host the platform on the system. Cloud platforms provide prefab functionality such as user interface, user sign up and administration, role based security, multi tenanted data management etc. [2]

c. Software as a service (SaaS):

The most important and most visible of the three is software cloud without which there is no need of platform or infrastructure. [4]

In purist sense a software cloud is the one which refers only to that software which intentionally which takes the advantages of both the other clouds namely: Iaas and Paas.

III. SECURITY ISSUES AND CHALLENGES

A. Security Concerns of Cloud Computing

Cloud computing is basically computation of data over internet. And so security of data present over cloud is the major concern of an IT company as data is the most crucial asset of any organization. [9]

- The most basic issue in cloud is that the data does not reside in physical location, instead the data is abstracted and scattered over the virtual servers.
- The access of data is the next concern of any organization. Who has the access and how he is going to utilize it? Is the data secure or not? These are the basic concerns of any organization.
- The next issue faced by any organization is the validity of the service provider and the assurance of long term secure management of data.
- Disaster recovery is also one of the major concerns of any organization before investing into any cloud service.
- The customers are also keen to know that how the service provider will take care of all the attempts to breach the security.[9]

B. Cloud Computing Attacks

a. Man in the middle attack:

If a third person gets access to the user's password he may easily get access to the crucial and confidential data present on the cloud. Also the communication can be changed and the original data can be lost.

b. Authentication attack:

c. Denial of service attack:

Some professional think that clouds are more vulnerable to DoS attacks, because it is a shared medium between multiple users and thus making it easier to suffer with DoS attacks. [1]

d. Side chain attack:

An attacker could attempt to place a virtual cloud is nearby approximate distance from the original cloud server and perform the side chain attack.

C. Fundamental principles for designing a cloud

- a. Least privilege: Least privilege to the attackers for attacking the cloud and breach the security.
- b. Defense in depth: The architecture must designed in such a way that there exists a level of security beneath each level of security to ensure that if one level is being breached by the attacker he is still not able to access the confidential data.
- c. Weakest link: The risky links or weakest sources in the system must be properly examined and taken care of.
- d. Recovery from failure: These must exists some means to recover from failure so that the data is not permanently lost.
- e. Open designing: Professionals argue that to have public key cryptographic technique is much better than private keys as when many person analysis the same codes; the security system hence being developed is much stronger.
- f. Complete meditation: The system must ask for authentication each time the user is updating or manipulating any data. Verification of the request must be done start from the initial procedure till end procedure.[10]

D. Solution From Security Challenges

- The data must be encrypted before being uploaded on the cloud. Also the encryption must be done to insure the security of data after attacks.[5]
- The mechanisms must be implemented in such a way that the owner is able to manage and grant permissions for accessing the data.
- Heterogeneous classification of data must be done at logical end of the cloud.
- Backups are maintained of the crucial data before uploading it to the cloud also there must be not changes in the keywords in the backup data
- The overall consistency and integrity must never be challenged and data recovery, authentication, user protection must be prime concerns.[5]

E. Conclusion

Cloud computing is now very much evolved and being used by several organizations by multiple cloud service providers but there exists some security issues that need

computing provides numerous benefits like easy access , mobility and high network coverage and these services can help the customers to design a very successful business strategy. [5]

The cloud providers must insure that the consistency and integrity of the data being uploaded is maintained.

REFERENCES

- [1] Pankaj Sharma, cloud computing, 1st ed., katson publication: April 2013, pp. 103-116, 2-10.
- [2] Deepak puthal, B.P.S Sahoo , Sambit Mishra and satyabrata swain, "cloud computing features, Issues and challenges: A big picture," pp. 116-120, 2015.
- [3] Haibo Yang, "A Descriptive Literature Review and Classification of Cloud Computing Research"
- [4] Qi Zhang · Lu Cheng · Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", 2010.
- [5] R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", ICC-2015.
- [6] Kernal Based Virtual Machine, www.linux-kvm.org/page/MainPage
- [7] Cloud Computing Bible, 2011, Wiley Publishing, Inc., Indianapolis, Indiana, pg. 8-9
- [8] Peter Mell, Timothy Grance , "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, September 2011, Special Publication 800-145.
- [9] Arora Pankaj, Wadhawan C.Rubal, Er.Ahuja P.Satinder, 2012, "Cloud Computing Security Issue in Infrastructure as a Service", International Journal of Advance Research in Computer Science and Software Engineering.
- [10] Garima gupta P.RLaxmi, Shubhanjali Sharma, "Survey on Cloud Security Issues and Techniques" 2011.