ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cloud Computing and Security Challenges

Routhu Sreelekha
B.Tech Student,
Department of Computer Science Engineering,
Andhra University College of Engineering for women.

1.Introduction :

Cloud computing increases financial and outfitted benefits, which allows organizations to understand significant cost savings and speed up deploying new applications. Though, business benefits cannot be obtained from an organization without using latest data security tests created by cloud computing. Because of unidentified, multi-inhabitant nature of cloud computing, there are chances of attacking confidential information and vital resources.

But unauthorized rendering leads to theft of information. Even though, the user leaves the cloud space, his data continue if the cloud vendor does not reprocess the storage securely. In this paper, part 2 focuses on cloud computing, part 3 focuses on security threats of cloud computing, part 4 focuses on the actions of those threats and part 5 is the concluding part of the paper.

2.Cloud computing :

According to the definition of NIST, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

"Reuse of IT resources" is the basic idea to build cloud computing. The distinction observed when cloud computing is evaluated with conventional methods like grid computing, distributed computing, utility computing is to enlarge the possibilities from corner to corner in an organization.

2.1 Attributes of Cloud Computing:

2.1.1. Use on request:

A person at any time and from any place can use the resources via worldwide network. These resources can be accessed without the need for human intrusion.

2.1.2. Resource allocation:

Large number of simultaneous users are allocated with resources into such a way that the system dynamically deal out according to customer requirements. No control is given to the users over the physical parameters, but cloud solutions can choose where the data is stored.

2.1.3. Network accesses:

Users can access the network through different devices like smart phones, mobile device, computers, etc.

2.1.4. Quantifiable service and transparency:

These can mechanically control the resources depending on users' criteria. It provides transparency to both users and vendors by observing, controlling and reporting the resource usage.

2.1.5. Scalability, Elasticity, and Flexibility of the cloud:

Cloud has the biggest advantage of having these three properties. It has the capability in allocating the resources dynamically whenever it is necessary to guarantee a smooth flow of operation. The extra resources can be purchased by the user at any period in any extent.

2.2 Models of cloud computing:

2.2.1 SaaS: SaaS is referred as Software as a Service, where the software and its related data are hosted in the cloud and these are accessed by users using a thin client, like using a web browser. New releases are hosted without requiring user to install new software physically. SaaS has a single configuration, which makes development testing faster. It is a model of “Software delivery”.

2.2.2 PaaS:

PaaS refers to Platform as a Service. PaaS serves to develop, test, deploy, host and maintain applications in the same integrated developing environment. It provides computing platform and solution stack. It manages the necessary hardware and software. It deploys the application without any cost and complexity. It supports teamwork.

2.2.3 IaaS:

IaaS refers to Infrastructure as a Service. Rather than from a local computer, the user can access the logical computational resources via a computer network. Users can store and access files such as pictures, videos, music, etc on a remote server. This stage can be described as hypervisor.

2.3 Deployment models:

2.3.1. Public cloud:

Public cloud is accessible to everyone. In this, same infrastructure is shared by all the customers, where they are managed and maintained by the cloud provider.

2.3.2. Private cloud:

Private clouds are building up for a particular organization containing of multiple users. These have more security and privacy. It requires capital investment and experts to build and maintain.

2.3.3. Hybrid Cloud:

Combination of both public cloud and private cloud is hybrid cloud. Computing flexibility is increased. Maximum of workload is deployed on the private cloud. Resources available in public cloud can be used when there is overflow of resources in a private cloud.

3. Security risks in this paper we come across four types of security risks. They are

1) Data related security
2) Application related security
3) Network level attacks.

3.1 Data related security:

Cloud computing is reliant on internet technology. This can be considered as a major disadvantage of cloud computing because one can access the cloud only by internet connection. So we need to consider secure data transfer on a secure data channel.

1) Data Infringement
2) Data Location
3) Data recovery.

3.1.1 Data Infringement:

Data infringement refers as data breach which refers as an occurrence of unauthorized access or viewing or reclaim of data by an individual or application. We can describe it as making the data public in an unsecured or unauthorized location. We can reduce this by small techniques in the business world. Most of the companies allow the employees to use their own electronics in the office and work with them on company projects and they are able to access the Internet through office WiFi. This may infect the intranet as if any, personal device infected with viruses or malware. A good solution to this is, office need to provide electronic devices to do their job.Requires all employees to use strong password protection, it becomes difficult fora hacker to crack a device. Encryption needed to be installed on all devices used to send or receive sensitive data.

3.1.2 Data Location:

We do not know precisely where the data is hosted, when we use cloud. Actually, we might not know in which country it is stored. We need to ask providers to store and process data indefinite authority and need to have a commitment to act upon local confidential requirements as Gartner advises. This issue concern can also be worked out by creating protected SaaS model which provides consistency in the area of the data stored to the customer.

3.1.3 Data recovery:

Data recovery refers to the process of data backup and allowing systems to recover data due to loss of data. It involves copying and documenting computer data, in order that it can access, if data corrupted or deleted. Data recovery is a part of disaster recovery.

There may be a chance that server breaks down and it damages the customer's data. Data need to be backed up to avoid this by allowing users to synchronize their local documents with cloud account, so that they can be recovered in the future.

3.2 Application related security issues:

In this sector, we come across the cloud malware injection attack, cookie poisoning, backdoor and debug option related issues.

3.2.1 Cloud malware injection attack:

This attack is executed by developing malicious software and adding to the cloud system. Once it is added, attacker shows it as a valid occurrence to the cloud system. On success, user requests its service and it is executed. There are chances of hardware damage, if the cloud accepts the virus instance.In order to avoid it reliable checks need to be performed on requests. We can create a hash value for storing original source; thereby attacker needs to create valid hash value to add up malicious software in the cloud system.

3.2.2 Cookie poisoning:

Cookie poisoning is an unauthorized access of data in a cookie and retrieves some information. Concentrating on cookies to hack the data is referred as cookie poisoning. We need to clean up the cookie or encrypt data to avoid cookie poisoning.

3.2.3 Backdoor and debug option:

Debug option is generally used by the developers when they make website public. These sometimes act as a backdoor for the hackers and change the website, if the options are enabled unseen. Therefore, developer needs to disable the debug option to avoid this attack.

3.3Network level attacks:

The network level security enables data availability, integrity and confidentiality when data moves from or to an organization in public cloud architecture.

3.3.1 Replay attack:

Replay attack is a network attack, which involves transmission of valid data repeatedly for a service and gain access to unauthorized resources. We can easily detect this attack on web as payload information is available. We can detect the patterns more easily with the usage of right tools.

3.3.2 IP spoofing:

IP spoofing is making the IP address look like authentic by masking it. It is a process of taking control through a fake IP address. In order to prevent this, we need to organize firewall rules to monitor and filter out harmful traffic.

3.3.3 DNS attacks:

In DNS attack, attacker prevents the authorized user from accessing the service. In general, user knows domain name rather than IP address, because of this reason; he may route to some other cloud in preference he asked.

Security requirements in cloud computing:

In order to develop secure cloud system, we need to have these security requirements.

Confidentiality:

The avoidance of unauthorized access of information from harmful gatecrasher and allowing access to sensitive data for authorized users refers to confidentiality.

Integrity:

Integrity refers to safeguard the data from unauthorized user alteration. In cloud, integrity refers to avoiding modifications from an unauthorized users and avoiding modification of unauthorized data by authorized user.

Availability:

This ensures that the cloud services, Cloud data, computing resources are enable and manage when needed.

Authentication:

The process of ensuring and confirming a user's identity is referred as authentication. In cloud, we ensure authenticated user by the process of testing the user's identity.

Non repudiation:

The process of using digital signature between the parties assuring the message transmission. The key should not be public knowingly or unknowingly.

Challenges in Cloud Computing:

The world steps towards changeover to the cloud by increasing the value of business. This even changeover involves the benefits as well as challenges. The cloud computing is not open from issues like any new technology. Some of the important challenges are as follows.

Security:

Cloud computing also faces some security challenges in terms of data segregation, multi tenancy issue, authentication, sensitive data access, etc. Security also a challenge for the startup companies due to shortage of resources. Some of the solutions include cryptography, secure interfaces and legal support.

Therefore, one needs to understand the challenges in cloud system and develop solutions for the success of the budding model.

Service level agreement:

Service level agreement is a contract for new services and associations in the cloud system between cloud provider and customer. It is a relationship in measurable term. The challenge lies in the violation of agreement. Providers deals with melancholic customers, when it occurs. On breaking the agreement, the cost would intimidate company's profits.

Performance:

Cloud system must provide enhanced performance and the performance is evaluated by the applications ability in the cloud system. Users normally prefer to use more than one cloud. The data concerted applications challenges to provide suitable resources. Performance may result poor due to lack of good resources which may lead to poor service delivery.

Interoperability:

It refers to the property of uncontrolled distribution of resources between different resources. Cloud users have an ability to use the application across various cloud platforms. Lack of open standards and interfaces becomes a challenge for interoperability.

Resource management:

Resource management describes the efficient usage of resources. Different resource allocation approaches need to be followed in cloud system because it is a collaboration of different technologies. Different scheduling algorithms need to follow for resource selection, resource allocation and resource release. If this is not properly done, it leads to performance degrade and wastage of resources.

Conclusion:

One of the revolution in the world of computers is could computing. Cloud computing is expected to transform the landscape of IT industry. It has bright prospects in future, but it needs to address the certain issues like security, interoperability, performance, scalability, reliability, etc. In this paper, we discussed about attributes, service models and deployment models of cloud computing, security risks, security requirements and challenges of cloud computing. Data related security is the major issue and the paper also addressed the other issues like application related, network related, etc and solutions to prevent the attacks. Customers often concern about security in adoption of cloud. Cloud vendors need to inform to their customers about the security levels, they provide to cloud systems. It is required to develop new security techniques to work with cloud architecture along with improvements of old techniques. The further research work includes the design challenging issues in the architecture of cloud system.

References:

1. Recommendations of the National Institute of Standards and Technology, The NIST definition of cloud computing.

2. A research paper on Levels of security issues in cloud computing, by R. Charanya1, M.Aramudhan2, K. Mohan3, S. Nithya4.

3. A presentation on Security issues and challenges in Cloud Computing by Lambu Akhila Reddy.

4. Definitions from the website http://www.techopedia.com

5. Overview of cloud computing by Torry Harries.s