International Journal of Combined Research & Development (IJCRD)
eISSN: 2321-225X;pISSN:2321-2241 Volume: 4; Issue: 10; October -2015

Security Problems and Strategy in Cloud Computing

Mr. Lochan B.

Asst. Prof, Department of CSE,
SVCE, Bangalore, India

Abstract : Cloud Computing is a new technology that is mainly used for large computations workload for clouds. Security is the key factors in these computing. There are various advantages in the cloud computing that mainly leads to data storage, bandwidth, power and software that has been shared for the clouds. There are various models Grid, Parallel and Utility Computing are used .Characters such as Reliability , Expansibility and low price service been used. In these papers it mainly deals with how the security and strategy will be taken place in the cloud. In the cloud storage, only single security method cannot be used to solve the problems and it should contains a total computing and new technologies that are used in the Cloud Computing System.

I. INTRODUCTION

Nowdays, the Cloud Computing is used in both Industry and academics. Basically it is mainly used for data storage. Security is the key for the cloud computing. The users can use the data anywhere. There is a fast development in the cloud server that the services are used. The service provided by the cloud to the customers having high scalability and reliability. The cloud system are transparent for application that are used in the resources and customers will not be knowing where to place the data. As the technology improving , there is a change in the industry for the development of information that are used in the society. There are virtualization technologies are used in the server to store the data as a centre location.

It can access anywhere in the world includes applications, platform and business mode. The advantage of cloud computing is having high reliability and scalability. Resource are shared by many number of users. The data which are stored by the user are confidentiality. Hacker may use the different software to get the data. The company will be provided a server that is mainly used for storing the data . In these servers there are two things one is public and private. The private server that are access by only the people who are there in a company. But the public data which are used that can be access by any number of peoples. The data stored in public or private system it guarantee the security of the data which are not used by the other users in the system. Platforms are been provided by the most of the companies. There are various problems are used in the cloud computing. There is no boundary and mobility's been used in the cloud Computing these leads to many security problems. The main problems include security of data, protection of data depending on the platform and administration.

II. CLOUD COMPUTING

Cloud Computing means data storage not used in the local computer but there are used in the distributed networks across the networks. The cloud computing performs the operation in personal computer and it includes the data centre either in public data or the private data. When it is used in the private data centre it can distributed across the various large data centers. The cloud give good service quality, reliable it provides on demand service and it automatically capabilities are need. The cloud system infrastructures are owned by an organization which sells cloud services to the general public or to a large industry company. The public cloud is running in the internet and the security is very complex. The service can be given to machines such a computer ,laptop and mobiles.
It includes various service models Software as a Server (SaaS) mainly deals with server that are used based on the software. Platform as a Servers (PaaS) deals with application that are used in the configuration, Development, Testing and Deploying. Infrastructure as a Servers (IaaS) deals with infrastructure that are used in the servers.

Sharing of the resources may be network, database and through servers. Examples is Amazon Elastic Compute Cloud (EC2). Virtualization Techniques are used in the Cloud Servers.

The resources mainly include the hardware, service, software that are shared fully. In a single system, multiple operating system are running. A Server can be service the host if it is running in the correct environment there is no affected by a host. Host can be added or removed based on the accommodate maintenance. The cloud computing has three important types public, private and hybrid. The public cloud is mainly used to access by various external data centre .The private cloud is mainly used for accessing restricted centre mainly used for confidentiality in internal data centers. The hybrid cloud is the combination of one or more clouds. It mainly consist of two sections one is front end and other is back end. The front end is the user or customer and back end is the resource or service provided by user. It includes various technologies. The Grid Computing is used for solving the problems based on resource, Cloud Computing is mainly used for allocation or sharing of the resources, Parallel computing is mainly used for performing the two or more computing operation at a same time. There are various cloud computing that are used in the market like Google, IBM etc. In Google it mainly consist of Google File System(GFS) which are distributed file system contain one master and any number of servers. The MapReduce operation are used. In these two operations to be performed. It maps the keys value and reduces the key and values are used. It performs the operations or the tasks and integrates the results. The MapReduce is used in the scheduling model not only in programming mode. The Bigtable depends on group of scheduling to perform the operation.The BigTables are used in the Database management systems which mainly include the tables. The Hadoop Distributed File System(HDFS) it works based on master-slave operation it contain center server i.e name nodes and manages the data i.e data nodes. The applications can be extended as the number of user increasing.

III CLOUD SECURITY PROBLEM

Internet is the most things that is used for running the cloud system and problems are also found in the internet. Some of the security problems consist of virus that leads to data lost. Hackers leads to the hack the cloud account and steal the data in the system. The cloud system is deployed for the security of the data. The cloud center includes the data and business application used for protection of resources. Cloud Computing is a technology is used to change the services, computing and virtualization includes the service, platform and application. The Cloud System mainly deals with Resource, Operation and Networks. If the system fails, the recovery of data is the problems. The system hides the operations or implementation services which are provided by the cloud. The key factors that are used in the user is the resource and privacy data. Data Integrity is used to change the data only authorized user and confidentiality means user can read the data. Transmitting the data through network leads to high flexibility and high scalability of the system to the user. The system in which data are stored deployed to different areas in different clouds nodes. Some of the accessing control are licensing, certification of cloud that are used in the data storage. In cloud computing there are many users changing the service needs. Position of data and how the servers are processing the data are the important problems that are facing by the users. The services must be improved with protecting of the data

IV. STRATEGY

In the Cloud system, whatever the data has stored it can be changed by someone or modified by the hackers. So Encrypting the data before deploying in the servers. The data size is small it will not be a problem if it is large, it takes extra time and resources. Security may leads to data storage, recovery ,availability ,survivability for the long term of the data. Data is stored in the cloud, the data can be transferred to the server or the cloud providers. The manipulation and data storage related to the resource mainly leads to the environment. The services offered by customers is difficult to get full transparency. Internal process of cloud computing and storage location of the cloud may do not know to the customer. The data how it gets fails with the cloud the customer may not know. The customer should be carefully check the services with security given to the data. The technologies include Confidentiality, Authentication, Integrity, Non-Repudiation, Availability and Access Control. The difficulty of decryption mainly depends on encryption. It also includes asymmetric key, symmetric key in the encryption methods. Authentication is mainly used to solve the problem of cloud security. In real time, traffic and status can be monitored. The unwanted network will be detected and they are fixed. The interruption and failures may leads to the hackers. There should be improved in the response and

capabilities mechanisms. Data security recovery and data backup is important for the customers. The availability, security and integrity may be protected to the user information.

The virtual private network and encryption can be used for the data transmissions. The user which are connected to cloud server may provide an operations to the user, maintenance, operation and various tasks are carried on . Transmitting the data one server to the server user don't know what is the data storage place. Trojan, virus may affect the internal and external controller in the cloud computing platforms. Damage to the system should be repaired fast so that the backup data should not affect. Designing Encryption and Key distribution mechanism should be proper. The system may provide service architecture in which details and services are hidden to customers. The services can be used as web service for the reference. Different system may use different programming language for the different application, for different platforms through the protocols. The services can be trust, secure conversation and authorizations.

V CONCLUSION

This paper illustrate the problems of cloud security. Backup ,Recovery of the data, Integrity and authentications are the principles used in the cloud computing. It relates to many service and managements. The data privacy is more than the traditional networks depending on the environment, platform and servers. Many customer may misuse the data, the security for the data are shown in these papers. There is a public and private clouds are also used to solve the problems. The main discussion is the security problems in the cloud computing. There are many users in which how data can be protected without any modification or changes done by the other user. Encryption such as symmetric and asymmetric keys and Decryption is used.

VI REFERENCE

[1] Amazon Elastic Compute Cloud, http://www.amazon.com/ec2/
[2] Google App Engine, http://appengine.google.com/