DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5556

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

CLOUD COMPUTING: A FOCUS ON SECURITY ISSUES IN CLOUD COMPUTING REGION

Er. Amandeep kaur
Assistant Professors
Department of Computer Science, Baba Farid College,
Bathinda, Punjab, India

Ramandeep kaur
Assistant Professors
Department of Computer Science, Baba Farid College,
Bathinda, Punjab, India

Abstract: Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services Limited control over the data may have various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. In this paper, firstly we have given introduction about security in cloud computing and then we discuss various models of security and solutions of cloud computing security. Further, data security challenges explored and data security solutions have been discussed at the end.

Keywords: CSP, ISP ,Cloud Computing, Iaas, paas, Saas

1. INTRODUCTION

Cloud computing is an IT based Technology that provides convenient on-demand network access to a shared configurable computing resources such as networks, servers, storage, applications which can be rapidly provisioned and requires less management effort or service provider's interaction. Cloud computing is reviewed concept that is originated from the earlier one distributed computing technology. However, it will be a subversion technology and cloud computing will be the third revolution in the IT industry, which represent the development trend of the IT industry from hardware to software, software to services, distributed service to centralized service. Cloud computing is also a new mode of business computing, it will be widely used in the near future.

Cloud Computing is based on distributed architecture in which server resources are centralized on a scalable platform to provide on-demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms that helps their customers to use and create their own web services, such that internet service providers offer costumers high speed broadband to access the internet services. CSPs and ISPs (Internet Service Providers) both offer separate services. In some cases, stored sensitive data at remote cloud servers are also to be counted. Security has been at the core of safe computing practices. When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns.

2. CLOUD COMPUTING'S MODEL

Cloud computing services are categorized into three pars: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)[1].

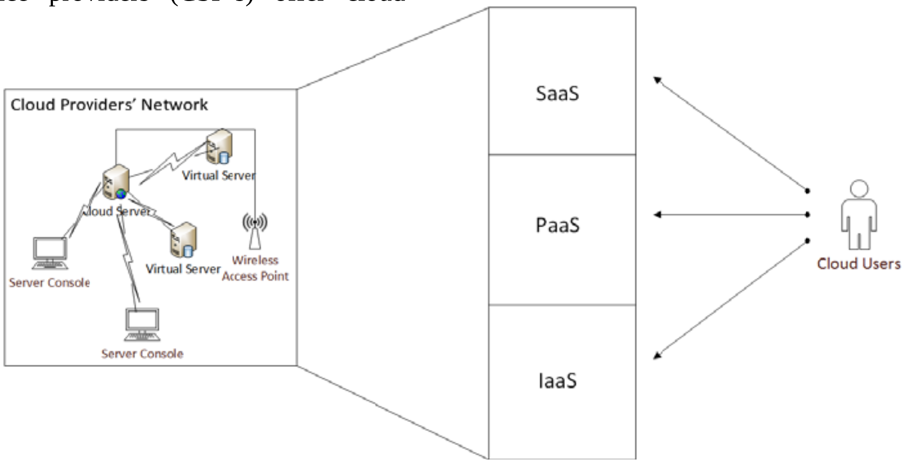

Figure 1: Cloud computing Service

2.1 Software-as-a-Service (SaaS): SaaS can be described as a process by which Application Service Provider (ASP) provides different software applications over the Internet. [3]. Cloud consumers work in hosting environment by releasing their applications which can be accessed from various clients by application users through networks.

2.2 Platform as a Service (PaaS): PaaS is a development platform that supports the“Software Lifecycle” completely which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. “PaaS provides a computing platform and solution stack as a service without the help of software downloads or installation for end users, developers. For Example : Force.com, Google App Engine and Microsoft Azure.

2.3 Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) concerns to the sharing of hardware resources for executing services using Virtualization technology. Virtualization is extensively used in IaaS cloud that refers integration or decomposition of physical resources in an ad-hoc manner to fulfill growing or shrinking resource demand from cloud consumers. The main objective is to make more readily accessible to thr resources such as servers, network and storage by applications and operating systems. [2]Examples of IaaS is Amazon Elastic Cloud Computing (EC2),Go grid, Amazon S3 .

3. DATA SECURITY CHALLENGES

As we are moving into internet based cloud model, it requires great emphasis on Data Security and Privacy[3]. Data loss or Data leakage can have severe impact on business, brand and trust of an organization. When multiple organizations share resources there is a risk of data misuse. So, to avoid risk it is necessary to secure data repositories and also the data that involves storage, transit or process. Protection of data is the most important challenges in cloud computing. To enhance the security in cloud computing, it is important to provide authentication, authorization and access control for data stored in cloud. The main areas in data security are

3.1 Confidentiality: - Top vulnerabilities are to be checked to ensure that data is protected from any attacks. So security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms etc. When data is stored on the remote server, data confidentiality is very important. To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility[3].

3.2 Availability: - Availability is the most important issue in several organizations facing downtime as a major issue. It depends on the agreement between vendor and the client.

3.3 Locality

In cloud computing, the data is distributed over the number of regions and to find the location of data is difficult. When the data is moved to different geographic locations the laws governing on that data can also change. So there is an issue of compliance and data privacy laws in cloud computing. Customers should know their data location and it is to be intimated by the service provider.

3.4 Integrity

The system should maintain security such that data can be only modified by the authorized person. In cloud based environment, data integrity must be maintained correctly to avoid the data lost. In general every transactions in cloud computing should follow ACID Properties to preserver data integrity. Most of the web services face lot of problems with the transaction management frequently as it uses HTTP services. HTTP service does not support transaction or guarantee delivery. It can be handled by implementing transaction management in the API itself.

3.5 Data Access

Data access refers to the various policies of data security. In an organization, the employees are given access to the particular section of data, based on security policies of their company. And that same data cannot be accessed by the other employees of the same organization. Various encryption techniques and key management mechanisms are used to ensure that data are shared only with the valid users. The key is distributed only to the authorized parties using various key distribution mechanisms. To secure the data from the unauthorized users the data security policies must be strictly followed. Since access is given through the internet for all cloud users, it is necessary to provide privileged user access. User can use data encryption and protection mechanisms to avoid security risk.

4.SOLUTIONS TO DATA SECURITY CHALLENGES

Encryption is suggested as a better solution to secure information. Before storing data in cloud server it is better to encrypt data. Data Owner can give permission to particular group member such that data can be easily accessed[4] by them. A data security model comprises of authentication, data encryption and data integrity, data recovery, user protection has to be designed to improve the data security over cloud. To ensure privacy and data security data protection can be used as a service. To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered. This hash calculation can be used for data integrity but it is very difficult to maintain it. RSA based data integrity check can be provided by combining identity based cryptography and RSA Signature. SaaS ensures that there must be clear boundaries both at the physical level and application level to segregate data from different users.[3] Distributed access control architecture can be used for access management in cloud computing. To identify unauthorized users, using of credential or attributed based policies are better. Permission as a service can be used to tell the user that which part of data can be accessed. Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents. A data driven framework can be designed for secure data processing and sharing between cloud users. Network based intrusion prevention system is used to detect threats in real-time. To compute large files with different sizes and to address remote data security RSA based storage security method can be used. [4]. These solutions will lead to more secure cloud storage, which will also lead to more acceptance from the people and the trust on the cloud will increase.

5. CONCLUSION

In this paper models of cloud computing, data security challenges and solutions are provided. In future concrete standards for cloud computing. Security can be developed. To provide a secure data access in cloud, advanced encryption techniques can be used for Storing and retrieving data from cloud.

REFERENCES

1. Ahmed and Hossain,” Cloud Computing And Security Issues In The Cloud”, International Journal Of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
2. Ali ,Khan and Vasilakos,” Security in cloud computing: Opportunities and challenges”,Information Sciences 357–383 ,2015
3. Padhy, R. P.,”Cloud Computing: Security Issues and Research Challenges.”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) , 136-146.2011
4. Aldossary and, Allen,” Cloud Computing: Issues and Current Solutions”, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016