IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Survey On Security Threats In Data Storing & Sharing In Cloud Environment

Seema Tahalyani[1] and Dr. S.M Ghosh[2]

[1] CSE Department, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India

[2] CSE Department, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India

Abstract

Cloud Computing is a next generation model which has gained popularity in recent years. Cloud computing paradigm is based on Internet that provides various provisions like sharing of configurable computing resources, on demand services any where any time and at any place across the globe. A key trait of cloud computing services is outsourcing and sharing of user's data. Cloud provides the facility of huge amount of storage space for data but at the same time users doesn't have the authority to control the outsourced data. In the shared tenancy system like cloud various security concerns regarding data storing and sharing arise which are major issues of concerns. In this paper, we are going to present an analytical study of cloud computing model and throw light on various services provided by cloud. Further we are going to focus on several security threats that arise during data storage and data sharing in cloud.

Keywords: *Cloud computation, Service Models, Deployment model, reference architecture, data security, and data sharing.*

1. Introduction

Cloud computing model is a next generation paradigm for IT industry. Cloud computing model use computer technology and is entirely based on Internet without which its existence become impossible. Its architecture contains large data centers that are converted into pools of computing resources. Storing data into cloud is a convenient way for the users to get rid from the complexity of hardware and other resource maintenance and management. The customizable computing resources are made available to the users as per their need by the Cloud Service Providers (CSP). In other words, one can access anything through cloud from anywhere from any place and from any computer on a per use basis [1]. The vision that various utilities based services made easily available to the users on the basis of on demand usage is an innovative concept. Cloud computing platform hides the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface). The computing resources may be networks, hardware and software, servers, storage devices, applications etc. Figure 1.1 shows how various resources are connected in the cloud for sharing purpose. Cloud has the property of elasticity which means pay only for those resources that are needed [2].

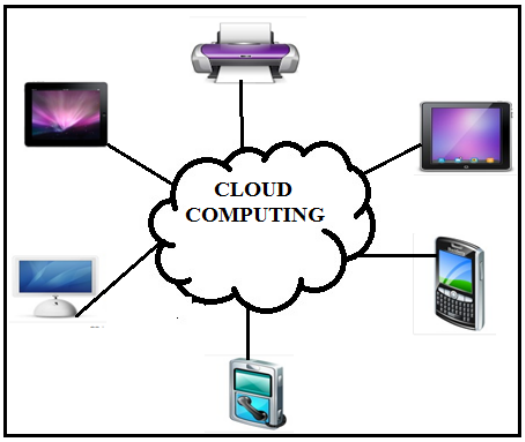

Fig. 1 Sharing of various resources in cloud computing

Evolution of Cloud Computation is still going on and there is no widely accepted definition of it. But according to NIST (National Institute of standards and technology) cloud computation is defined as [17]:

"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."

Some essential characteristics of cloud that make it unique in comparison to other traditional technologies are [2]:

- On-demand self services
- Broad network access
- Resource Pooling
- Rapid elasticity

ISSN 2348 – 7968

- Measured Services

Thus providing many benefits to the business enterprises and attracting them to move towards it.
Some benefits provided by cloud computation is shown in Table 1.

Table 1: Benefits of cloud computing

Scalable and Flexible	Disaster recovery
Automatic software updates	Free Capital expenditure
Increased participation	Competitiveness
Work from anywhere by improving accessibility	Resource allocation time reduction
Environmentally friendly	No need to buy expensive software
Personnel training are not required	Pay for what you use

Due to these reasons cloud is becoming demand for the present business scenario.

2. Cloud Models

Cloud computing in alliance with Internet yields many IT services to its users that can be configured by the customers according to their needs and requirements. Scaling of services over network reduces the cost and helps in managing data efficiently. These services are provided by a Cloud Service provider (CSP) to the customers based on Service Level agreement (SLAs). Basically there are two types of cloud models: Service Models and Deployment Models [17].

2.1 Service Models

Cloud computing provides many facilities in the form of services (***as a service***) to the various client with the help of Internet. These services reflect different aspects of cloud computing paradigm at different levels of framework [4]. At a higher level, clouds can be viewed into three levels of services- IaaS, PaaS, SaaS

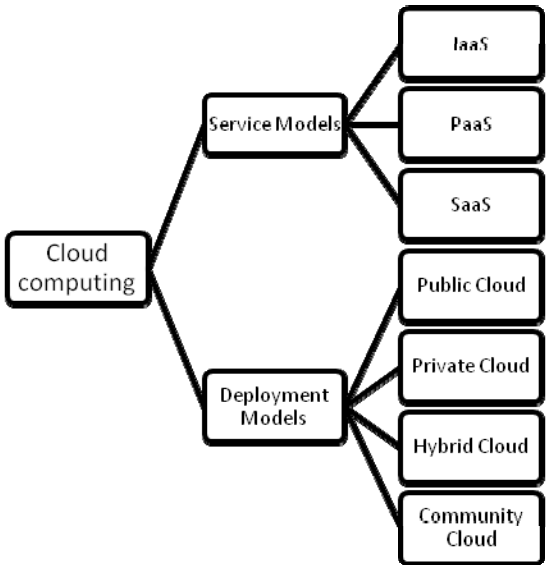

Fig.2 Cloud computing model

Infrastructure as a Service (IaaS):

Virtualization is the main concept behind the cloud computing model. Infrastructure as a Service (IaaS) facilitates virtualized platform, virtualized servers, networking and storage devices and other fundamental computing resources to the customers. Without actually purchasing these resources customer can use them just by paying the rental amount of resources they want to use. Consumer gains infrastructure from this service, over which they can install any platform. Allows users to deploy and run random software and applications. Amazon EC2, Windows Azure, Rack space, Google Compute Engine are some instances of IaaS. IaaS may be further categorised into two sub services:

- Storage as a service (StaaS) :
  This service permits users to store their data at remote server and devices. Some StaaS service providers are: AmazonS3, Amazon EBS etc.
- Compute as a Service: Some IaaS computing services are: AmazonEC2, Layered tech and so on.

Platform as a Service (PaaS):

Platform as a Service model provides software framework to software developers to deploy their applications. As the name refers it provides platform where applications can be built, hosted tested and deployed easily. Consumer does not have to manage the underlying infrastructure. Examples of PaaS are: Google App Engine (GAE), Microsoft Azure, IBM Smart Cloud, Amazon EC2, salesforce.com and jelastic.com billing services provided

ISSN 2348 – 7968

by Arial system, op source; Financial services: Concur, workday, Backup and recovery services and so on, Google Docs, SAP business by design and so on.

Software as a Service (SaaS):

Software as a Service provides those services to the consumer which are developed and managed by third parties or vendors. With SaaS, applications can be used with the help of a web browser without installing them directly. This reduces the management and maintenance cost of business enterprises. Everything is managed by the vendors of SaaS. Clients only have to create an account to the vendors providing cloud services and use the specific functions provided by the cloud vendors. Rather than facilitating cloud features directly to a consumer they provide services and application using cloud platforms and infrastructure. Examples for SaaS include Gmail, Google Apps, Microsoft Office 365, Google+, facebook, yahoo, SalesForce.com etc.

2.2 Deployment Models

One of the important and popular usages of cloud is its storage capability. For the purpose of storage cloud can be broadly classified into four categories. This categorization is based on the nature of cloud, its purpose & its location and how cloud infrastructure is managed. The four categories are: Public cloud, Private cloud, Hybrid cloud and community cloud.

Public Cloud:

Public cloud storage is sometimes also known as external cloud storage. As the name suggest it is the service which can be used by any consumer that is it is openly accessible to the consumer. Public cloud storage providers provides infrastructure as a leasable commodity. Some of the leading public cloud providers are Amazon, Google App Engine and Microsoft Azure. One of the limitations of public cloud storage is that since it is authorized and managed by the third parties security becomes an important issue of concern.

Private Cloud:

Private Clouds are also known as “Internal cloud storage”. Private clouds are the cloud storage privately owned and managed by an enterprise or any user. As a private property, private clouds have premises and surrounded by the user’s firewall thus providing protection to the stored data. Only the authorized user can access the infrastructure and services under private clouds. Private cloud storage providers are Para scale, IBM, Clever safe and Eucalyptus Systems. It is more expensive but more secure than public clouds.

Hybrid Cloud:

Hybrid cloud models are also known as Virtual private cloud models. Hybrid cloud is the combination of private and public cloud. Hybrid cloud storage defines policies for the storing data. In other words, which data must be maintained privately and which should be maintained publicly. Hybrid cloud environment is hosted by third parties and some resources are publicly accessible and some are only accessed by the organization. Data transfer can take place between public and private clouds without affecting each other. Only limitation is creation and governance of this type of cloud model. Hybrid cloud providers include Amazon Web Services and Egnyte.

Community Cloud:

Community cloud models are the clouds in which infrastructure and services are shared and managed by a group of organization of common interest. These types of clouds are managed by third parties and are based on the legal agreement between organizations. Facebook is the most common and popular example of community cloud model.

3. Cloud Computing Reference Architecture

Reference architecture of cloud computing is a conceptual model that describes the needs, composition and operations of cloud computation. It defines the needs and requirements of services that cloud service provides. Reference architecture can be described as a tool for developing a system architecture using a common framework. Cloud computing Reference architecture has five main actors as shown in Figure 3 that play their roles in cloud environment and help in illustrating the concept of cloud computation. These five actors are: Cloud consumer, cloud provider, cloud auditor, cloud broker and cloud carrier. Their roles and responsibilities are as follows:

Cloud Consumer: Cloud consumer can be a person or an enterprise that ultimately going to use cloud services. Cloud consumer takes services from cloud providers.

Cloud Provider: Cloud Providers may be a person or an organization that provides services to the cloud consumer according to their requirements. The main activities of

ISSN 2348 – 7968

cloud providers are service deployment and orchestration, service management, security and privacy etc.

Cloud Auditor: They are the third independent parties that do the assessment of services provided by cloud providers. They also check the performance of cloud computing implementations.

Cloud Broker: Sometimes integration of cloud computing services becomes very complex. Cloud broker plays a vital role to manage these complexities and in maintaining the performance of services provided by cloud providers to the cloud consumers.

Cloud Carrier: A cloud carrier plays the role of negotiator that facilitates connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication, and other access devices.

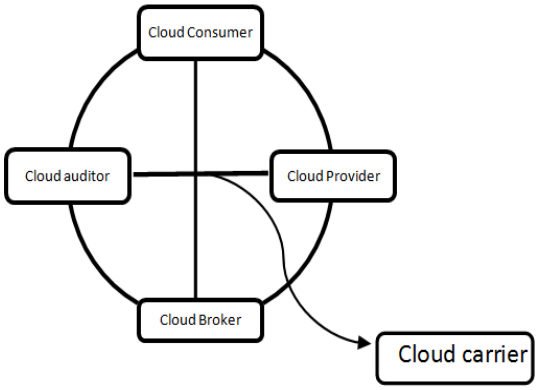

Fig. 3 Cloud Computing reference architecture

4. Storing and sharing data in the Cloud environment.

One of the prominent applications of cloud computing is outsourcing of data. A large amount of data can be stored in the Cloud and user is rid of the data management problem. Data in the cloud may be manageable or unmanageable.

4.1 Manageable Cloud Storage:

In managed data storage, various options like formatting, replicating data are provided. A raw virtualised disk is provided which is used for storing cloud based applications. They are mainly used by the developers. IaaS web services like applications, uses managed cloud based storage. Managed cloud storage providers are Amazon S3, Google Storage for developers, IBM Smart business Storage Cloud etc.

4.2 Unmanageable Cloud Storage:

Unmanaged cloud storage has a pre-defined disk drive and user have very limited control over the disk drive. They are cheap and easy to use cloud storage. SaaS web services like applications, uses unmanaged cloud based storage. Some services which uses unmanaged cloud storage are Dropbox, Adrive and 4Shared etc.

Data Sharing is another important aspect of cloud computing According to a survey now-a-days most of the organizations share their data with the help of a cloud. This reduces the cost, increase in productivity and distribution factor also improves. Most popular data sharing applications are social networking sites which are used to share text, photos, videos and events etc. the data in such type of environment changes rapidly with time. Data sharing has many merits and in some case causes have many harmful effects. As an instance if a document is shared it can help many students, and help a patient to get best medical advices. But if the cloud storage is used by some unauthorised user then it can hinder the privacy and security of any sensitive data. Many security concerns are discussed in next section.

5. Security Threats in Cloud

As a coin has two faces and one cannot be separated from other, similarly Cloud computing also has two inseparable faces one is its merit and other is its demerits. Above we had a brief view over its merits now we are going to have brief discussion on its limitations. The most important drawback of cloud computation is security and privacy issues of data stored. This section presents a review on the related work done to carry out in securing and data sharing aspect of cloud. *Xiao et al* [11] in his work has identified five major security concerns: confidentiality, privacy, availability, integrity and accountability. *Chen and Zhao* in his work described the necessity and requirements for secure data sharing in cloud environment. *Wang* [14][15] explained in detailed about the privacy and security of SaaS (Software as a Service) using pilot testing and security compliance. *Zhou* [13] explained in his survey about the laws for privacy and security; and how they can be considered while working in cloud environment. Some of the major threats [22] in cloud are shown in table 2.

Table 2: Some threats in data storing and sharing in Cloud environment

ISSN 2348 – 7968

S.No	*Security Threats*	*Explanation*
1	Data availability	Since a third party is involved in storing and sharing process sometimes it is difficult to believe over third party.
2	Data confidentiality	Extra efforts and measures is required for storing highly sensitive data in shared tenancy like cloud.
3	Data privacy	Data privacy can be harmed if unauthenticated users or any unexpected privileges act over data stored in cloud.
4	Data integrity	As users doesn't know where the data has been stored in cloud environment so there is chance of data being corrupted.
5	Shared tenancy environment	Virtualization is the basic key concept in cloud. An unauthenticated access may harm stored data.
6	Decentralized architecture	As authority is transferred from remote to local system may cause protection inconsistency.
7	No control over data stored	In cloud users doesn't have control over data as a result governance over data is lost.
8	Discontinuity in service delivery	Cloud provides sharing of pools of resources as a service and if these services gets discontinuous or delayed it may harm business.
9	Trust Loss	Since cloud has black box feature, it becomes difficult for users to measure the trust level of CSP.
10	Service Provider / Supplier Lock-in	Difficulties cause due in change of cloud service providers.
11	Unsecure cloud user access	Attack through unsecure Application Platform Interface(APIs).
12	Unclear definitions responsibilities	Unclear definition of services provided by CSP(Cloud Service Providers) and consumers may cause conflicts between them.
13	Lack of cryptographic management	Loss of cryptographic keys can cause loss of sensitive data.
14	Risks of license	Licenses of software are dependent on numbers of consumers installed that software may cause conflicts in software use.
15	Conflicts in law of countries	Different countries have different laws which can cause legal issues in protection of private data.

Conclusion

Cloud provides many services out of which data outsourcing and sharing is one of the important and advantageous aspects of it. Virtualization helps cloud to achieve many higher goals such as elasticity, reduction in cost, sharing, flexibility in services etc. But data security is one of the important issues of concern that has to be tackled while storing and sharing data over cloud platform. So there is a need to keep an eye over the security concerns while working in cloud environment especially if data is highly sensitive. In this paper, we have a briefly described various services and merits of cloud computing and focused on some of the threats that can harm storing and sharing process through cloud.

References

[1] V. Spoorthy, M. Mamatha, B. Santhosh Kumar, "A Survey on Data Storage and Security in Cloud Computing",IJCSMC, Vol. 3, Issue. 6, June 2014, pp.306 – 313.

[2] S V.Nandgaonkar, A. B. Raut, "A Comprehensive Study on Cloud Computing", IJCSMC, Vol. 3, Issue. 4, April 2014,pp.733 – 738.

[3] K.Lee, " Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications,Vol. 6, No. 4, October, 2012.

[4] R. B.Chandar, M. S. Kavitha and K. Seenivasan, "A proficient model for high end security in cloud computing", ICTACT Journal on soft computing, vol. 04, issue: 02 697, January 2014.

[5] D.Chen, H.Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012,Vol. , pp. 647-651.

[6] S.Sharma, A. Chugh, "Survey paper on cloud storage Security", IJIRCCE, Vol. 1, Issue 2, April 2013.

[7] R. P. Padhy, M. R. Patra, S.C. Satapathy, "Cloud Computing: Security Issues and Research Challenges", IRACST-(IJCSITS), Vol. 1, No. 2, December 2011.

[8] Sh. Ajoudanian and M. R. Ahmadi, "A Novel Data Security Model for Cloud Computing", IACSIT International Journal of Engineering and Technology, Vol. 4, No. 3, June 2012, pp 326-329.

[9] A.Ukil, D. Jana, A. D. Sarkar , "A security framework in cloud computing infrastructure", IJNSA, Vol.5, No.5, September 2013,pp 11-24.

[10] M. Ahmed and Md. A. Hossain, "Cloud computing and security issues in the cloud", IJNSA, Vol.6, No.1, January 2014.

ISSN 2348 – 7968

[11] Z. Xiao , Y.Xiao, "Security and privacy in cloud computing", IEEE Commun Surveys Tutorials 99:1–17, 2012.
[12] D. Hen , H. Zhao, "Data security and privacy protection issues in cloud computing", International conference on computer science and electronics, engineering,2012, pp 647–651.
[13] M. Zhou , "Security and privacy in the cloud: a survey", Sixth international conference on semantics knowledge and grid (SKG),2010,pp.105–112.
[14] J.Wang,C. Liu, GTR Lin, "How to manage information security in cloud, computing",2011, pp.1405–1410.
[15] Y.Wang, "The role of SaaS privacy and security compliance for continued SaaS use", International conference on networked computing and advanced information management (NCM), 2011, pp:303–306.
[16] N.Oza, K. Karppinen, R. Savola, "User experience and security in the cloud-An empirical study in the finnish cloud consortium. IEEE second international conference on cloud computing technology and science (CloudCom), 2010,pp.621–628.
[17] P.Mell and T.Grance, "The NIST definition of Cloud Computing,"http://csrc.nist.gov/publications/ nistpubs/800-145, September 2011.
[18] Cloud security alliance, "the Notorious Nine: Cloud Computing Top Threats in 2013",http://www.cldsecurityAlliance.org/topthreat.
[19] L.Hardesty, secure Computers Aren't so Secure, MITPress,http://www.physorg.com/news176107396 .html,2009.
[20] L.Arockiam, S.Manikandam, "Efficient Cloud storage Confidentiality to ensure data security". Computer communication and informatics, 2014 international conference.
[21] B.Sosinsky, Cloud Computing Bible, Indianapolis, Indiana: Wiley Publishing Inc., 2011.
[22] H. Mahajan, N.Giri, "Threats to cloud computing Security", VESIT , International Technological Conference-2014 (I-TechCON), Jan. 03 – 04, 2014.