Data Security Issues in Cloud Computing

NayanYerate
Computer Science & Engineering Dept.,
VVPIET, Solapur.

RajaniSajjan
Computer Science & Engineering Dept.,
VVPIET, Solapur.

***Abstract* --As we are familiar that the cloud computing field is very vast and also its one of the potential field. It also has many advantages over the other storing fields. This is the only reason that the data is being migrating from the local storages to the public or the hybrid clouds. Due to some of the drawbacks the large enterprises or the critical data of the organizations are not moved to the cloud. The actual size of the cloud is much more and effective than we expect it. The data owners i.e. the cloud consumers need a high level of security regarding their data and the privacy concerns are also there. This is one of the issue that many consumers are not moving towards the cloud computing services. In this paper short but and effective analysis on the data security and privacy protection part is provided which is concerned with the data life cycle in cloud computing. The further part consists of the present work in this area. Finally the future work and the conclusion of this topic.**

Keywords: cloud computing, cloud computing security, data segregation, access control, data security, privacy protection.

I. INTRODUCTION

Regarding definition of cloud computing model, the mostwidely used one is made by NIST as "*Cloud computing is amodel for enabling convenient, on-demand network access to ashared pool of configurable computing resources (e.g.,networks, servers, storage, applications, and services) that canbe rapidly provisioned and released with minimal managementeffort or service provider interaction. This cloud modelpromotes availability and is composed of five essentialcharacteristics, three service models, and four deploymentmodels.*"[2] The cloud computing model NIST defined hasthree service models and four deployment models. The threeservice models, also called SPI model, are: Cloud Software as aService (SaaS), Cloud Platform as a Service (PaaS) and CloudInfrastructure as a Service (IaaS). The four deployment modelsare: Private cloud, Community cloud, Public cloud and Hybridcloud[1].

There is a lots of difference between the initial stage and the todays condition of cloud computing. Its an more mature and grown up version in the todays scenario. The view of the business people is being changed they have understood the benefits of putting their data and applications on the cloud. All the small and medium business enterprise are relying on the cloud computing. The adoption of cloud computing is making the work more effective and efficient in developing and deployment and saving the cost in purchasing and maintaining the infrastructure.

Cloud computing has many efficient and effective plus points over the traditional IT computing models. The security of data is the major part which many of the data owners think and they find a problem in security and they do not go for cloud computing. Many of the surveys have proved this that due to security concern the people don't trust or use cloud computing. Data privacy is also one of the points.

But though the cloud computing service providers give an guarantee that they provide a major security and privacy to their data but its not the case actually. We cant easily rely on these thoughts. Major and famous cloud computing vendors had an security issue in 2009. Amazons simple storage service was interrupted in February and July 2009. This incident showed that the site was relying on a single storage service. Also in March 2009 Google Docs lead to an leakage of users private data. Google Gmail also had a failure for 4hours. If these kind of vulnerability appears in the VMwares then some destructive minds can take advantage of it and the situation will be worsened. A breach in the security policy of cloud computing may lead in the collapse of the entire cloud computing vendors. If the administrators loose upto 45% of data then the cloud computing LinkUp needs to be closed.

The traditional IT and cloud computing security issues are same. But this kind of security majors may lead to different risks and challenges in the cloud computing.

Then also the cloud computing environment uses the same security issues as that of traditional IT environment. As many of the enterprises are involved in the cloud computing the boundaries of the clouds need to be shifted from the traditional environment to the need of cloud computing environment. The cloud computing is bringing an major pressure on the security issue of the data this is due to the openness and the multi-tenant characteristic of the clouds.

a) As the clouds are dynamically scalable, service abstraction and location transparency features of cloud computing models all the applications and data on the cloud platform have no fixed infrastructure and security boundary. Due to this problem if there is a threat in the system then we can't decide that any of the hardware resource or any other part have created it.

b) In the service delivery model of cloud computing the security issue cannot be considered as the data is available on the multiple service providers. So a same model of security is not applicable to all the providers. The providers may have an conflict and a unique model is not possible.

c) As the openness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by other unauthorized users.

d) The cloud computing platform deals with the huge amount of information storage and provides quick access , cloud security measures need to meet a massive information processing.

In this paper we describe data security and privacy protection in the cloud. The paper consists of the following sections: section II describes the exact issues related to the cloud security, section III the data security and privacy protection issues are discussed by considering the entire phases of data life cycle. Section IV it contains the present results for data security and privacy protection in the cloud. Section V conclusion section VI future work.

II. SECURITY FACTS IN CLOUD COMPUTING

There are security issues in the cloud computing system. Some of the issues are discussed.

a) Security: Wikipedia[3] defines cloud computing security as "cloud computing security(cloud security) is an evolving sub-domain of computer security, network security and broadly information security. It refers to a broadset of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of cloud computing ". The cloud computing security is not cloud-based security software products such as cloud-based anti-virus, anti-spam, anti DDos and etc.

b) *Security facts tied with the cloud*

Many security facts are related with cloud computing and they are grouped in multiple views.

Gartner [4], made an statement that the whenever user makes a choice or have to choose an vendor certain safety and security measures need to be considered. The safety measures are : priority based user access, regulatory compliance, location of data to be placed, data collection, roll up or recover of data loss, support for investigation and long term viability. Forrester Research Inc. [5] major cloud providers security and privacy services are applicable in three areas: secure and private, requests made by people in the authority and obeying legal rules of the authority, and contract based facts. Some of the alliances have collected the solution providers, no profit no loss, and the expertise are involved so that the cloud providers will assure the information assurance in the cloud, this alliance is Cloud Security Alliance (CSA)[6].The CSA has realised thireen aspects of concern on cloud computing [7].

Many more investigations and research have been made by many of the researchers and scientists in the field of cloud computing and its security. Some of the protocols and algorithms are also designed for the security and privacy of the data on the cloud environment. Also an research have been made to increase the security in the case of architecture, service delivery models, characteristics of cloud and the stakeholders of the clouds. Some of the auditing protocols are also designed for privacy and security of the data in the clouds. There are far more opportunities in the field of cloud computing area.

The cloud computing security architecture can be divided into four different parts.

A) Security in software's
B) Security in the platforms
C) Security in infrastructure
D) Rules of the obeying the authority (auditing) and auditing

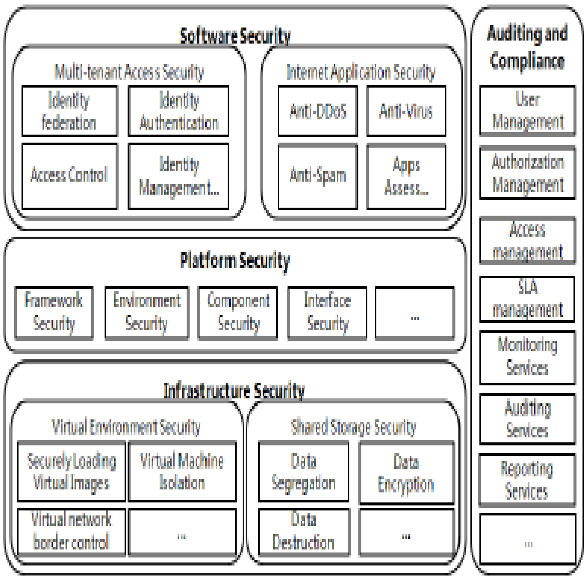

Figure1. Security architecture for cloud computing

III.DATA SECURITY AND PRIVACY PROTECTION FACTS

The traditional data security and privacy protection concepts are implemented in the cloud computing environment. Also its present in the each and every mode of data life cycle. As the cloud environment is multi-tenant and open characteristic of the cloud, the cloud computing security and privacy protection issues are having their own dimensions.

The term privacy is different for different countries, communities, organizations, and the jurisdictions. Different organizations have different definitions regarding the cloud security and privacy protection. OECD (Organization for Economic Cooperation and Development) has accepted a definition "any information relating to an identified or identifiable individual (data subject)". Some of the use to definitions are provided by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA).

The following part of the paper analyse data security and privacy protection facts in the cloud for the data life cycle stages.

1. Stages In Data Life

The first stage of data life cycle is to construct the data and the final or the last stage is to destroy the data. The diagram 2 shows the data life cycle .

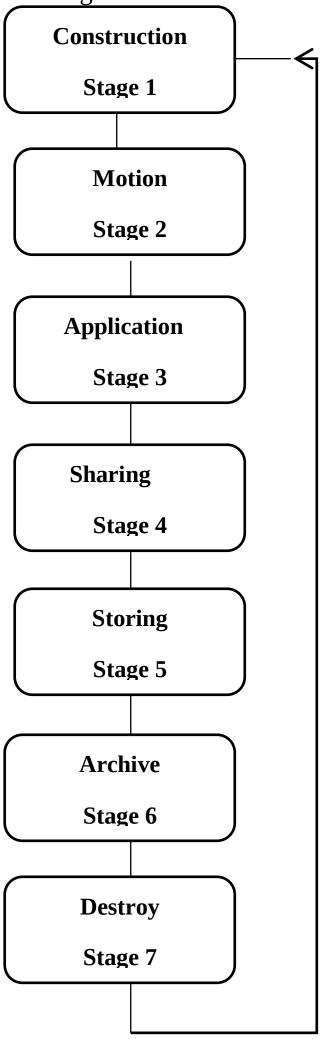

Fig2. Life Cycle of Data

A. Data Construction:

The data construction is done by the data owner. The users or the organizations or the enterprises manage and take hold of the data in the traditional IT environment. If the owner wish to transfer the data from the traditional environment to the cloud then different aspects need to be considered.

The personal and private data needs to be separated by the data owner itself.

B. Data Motion:

When the data nees to be transferred within the boundry line we don't need any encryption or only simple encryption is also done. Whenever we need to transfer the data across the boundaries then we need to take care of the data integrity and the confidentiality of the data. This should be done to avoid the data loss from being tapped or tampered. The unauthorized users access the data unethically and in turn owners loose their data.

C. *Application*

Mostly static data is used in the traditional IT environment and the cloud environment also. Some of the static data storages are Amazon S3 it is an simple and static data storage. Data can be encrypted in this type of application. PaaS and SaaS models are used in cloud based static applications. We cant use data encryption in each and every condition.the encryption has a problem of data indexing and quering. The static data which is encrypted is not used by the clouds. In cloud computing the data of different users is kept together so data encryption will create a problem. Unencrypted data may create serious problems in the cloud computing.

For private data the cloud computing has to deal with different issues. The data owners have to take a special care of the private and personal data, they need to consider if their data is being shared with the third parties or with some other service providers.

D. Sharing

Data sharing is extending the data ranges and using it on large extent. In the sharing process we need more data security and privacy concerns are also involved in this process. Also proper permissions are needed from the authority. When the data owner shares its data from one user to the other user then the next user can share the data of one user to other user without taking the permission of the data owner. The data owner have to take care of the data when the data is being shared and it have to rely on the providers. For data protection we can have different security measures like authorization and restricated access.

E. Storing

Whenever the data is stored on the cloud the data is divided into two catrgories

a) Amazon has an simple storage service named as laaS environment.
b) The cloud based applications have the Paas and SaaS storage facility.

The data stored in the clouds is similar to the data stored in the traditional IT environment. Whenever we store the data we need to consider the three important issues: 1) Confidential data 2) Data integrity 3) Data availability.

To maintain the data confidentiality we use data encryption technique. We use data encryption and key strength algorithms to maintain the data confidentiality. The encryption algorithms used in the cloud computing environment needs to be more fast and the computing speed should be increased even after using the encryption algorithms.

The key management is the major problem involved in the use of encryption. the key management is the responsibility of the data owners. The data owners are not expert in the key management so they are dependent on the cloud providers for the key management, but this increases the overload of the cloud providers and they need to manage the large amount of keys for different users.

Data integrity is also one of the important issue. Which needs to be considered. Data owners store a huge amount of data on the clouds but they are not sure aboutthe data integrity of the data as the data from the clouds is migrated and transferred from one location to another. Many of the processing is done on the data in the cloud computing.

The traditional IT data integrity concepts are not applicable to the cloud computing environment.

There are many attacks involved in the data security. Mostly the external systems have an external attack to breach the security of the data availability and integrity. In the cloud computing there are many other aspects also involved in the data availability also. A) cloud storage services provide the backup? B) cloud computing services available? C) whether the cloud computing services will be available in the future also?

F. Archiving

Archiving is mostly dependent on the media of storage. The storage duration and the storage media also plays an important role. If the media of the data storage is not reliable then there is a chance of data leakage.

G. Destroy

If the data is not used for longer time then the data is destroyed. But this leads to the loss of sensitive data.

IV. PRESENT RESULTS FOR DATA SECURITY AND PRIVACY PROTECTION

The homomorphic encryption developed by the IBM is the way of using the data without encrypting. This was developed in June 2009. [8]

The airavat system is a privacy protection system was developed by the Roy and Ramadan to control the flow of decentralized information and the differential privacy protection technology in data creation and calculation stages in the cloud. [9]. Privacy leakage is prevented by this system. The authorization is also not needed.

The data verification process is very lengthy as the data first needs to be downloaded, verified and then after verification needs to be uploaded. This takes a long time. And also It increases the time, cost and transfer fees is involved. The data owners find it very difficult. The dynamic data in the clouds cannot be treated same as that of the traditional IT environment data. The Cong Wang proposed a mathematical way to verify the integrity of the data dynamically stored in the cloud[10].

V. CONCLUSION

Cloud computing has a number of advantages over the traditional IT computing systems. But then to a lot of research and work is coming forward to remove all the vulnerabilities in the system and a lot of improvement is done in reducing the threats present in the system the vulnerabilities in the system, and the privacy protection.

As the data integrity and the privacy protection is an major issue in the cloud computing the steps are taken to solve these problems on priority.

Data security and privacy protection issue is related in all the stages of the data life cycle.

The major problem in the privacy protection is the sharing of data while ensuring the security regarding the private and personal data of the data owner.

The critical systems which need an acute security for the data security is the e-commerce in which the users credit card details are available and the health care systems have the very important health data of the patients and it needs to be secured. These systems need to be provided with the higher privacy protection and the data integrity. The websites can access the data and have the personal and private data of the concerned data and can misuse that data. But the present cloud systems do not assure that the personal information is secured from the third party.

When the design of the cloud computing we should consider the facts for privacy protection, private data identification and isolation.

VI. FUTURE WORK

Many of the algorithms and the protocols are designed and implemented in the field of cloud computing to enhance its features.

To protect the data and the privacy protection are the basic and the fundamental challenge for the separation of data which is sensitive and difficult to access. Our task is to design the unique identity management and a framework for privacy protection on the cloud computing environment. An authorization and un authorization of the users in an large organizations. This process needs to be more automated and dynamic to save the employees time in authorization and un-authorization process.

REFERENCES

[1] Deyan Chen and Hong Zhao “Data Securityand Privacy Protection Isues in Cloud Computing” , 2012 International Conference on Computer Science and Electronics Engineering.
[2] Peter Mell, and Tim Grance, “The NIST Definition of CloudComputing,” Version 15, 10-7-09, http://www.wheresmyserver.co.nz/
[3] Storage/media/faq-files/cloud-def-v15.pdf
Cloud computing security, ttp://en.wikipedia.org/wiki/Cloud_computing_security.
[4] Gartner: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.
[5] Cloud Security Front and Center. Forrester Research. 2009-11-18.

http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html

[6] Cloud Security Alliance. http://www.cloudsecurityalliance.org.

[7] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, http://www.cloudsecurityalliance.org/ guidance/csaguide.v2.1.pdf.

[8] "IBM Discovers Encryption Scheme That ould Improve Cloud Security, Spam Filtering," at http://www.eweek.com/c/a/Security/IBMUncovers- Encryption-Scheme-That-Could-Improve -Cloud-Security-Spam-Filtering-135413/.

[9] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E. "Airavat: Security and privacy for MapReduce," In: Castro M,eds. Proc. of the 7th UsenixSymp.on Networked Systems Design and Implementation. San Jose: USENIX Association, 2010. 297.312.

[10] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 7th
International Workshop on Quality of Service. 2009:1-9.