www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 6. May 2015

Data Security on Cloud

B.Kavirajan
Mary Matha College,
Periyakulam,Theni District

***Abstract*— It is essential that every company or organization has the right level of security to ensure they are free from the threat of danger, damage, theft or crime. if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but losing it to hackers or a malware infection can have much greater consequences.**

KeyWord : Destruction,Storage,Archival,Share,Transfer,Authorization,Authentication,Confidentiality,Consistency

I. INTRODUCTION

A. What is Cloud Data

Data Stored inside the cloud / cluster, which is monitor, managed by the organization or by cloud service provider.

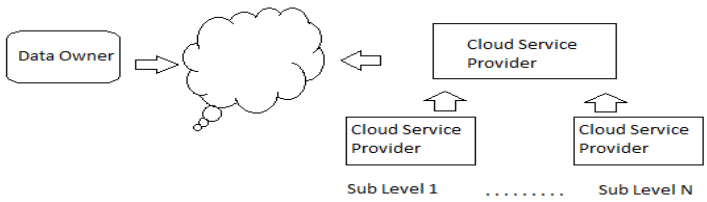
B. What is Cloud Data Security

Data stored inside the clusters need to be maintained and processed with high level security. It should maintain confidentiality and consistency in all levels**.** Only authorized persons can use the data. Data should be highly restricted to unauthorized persons. The following are the security parameters.

- Authorization.
- Authentication
- Confidentiality.
- Consistency.

C. How Data is handled?

Data owner / organization move or share their data in to the cloud through cloud service provider. Here the cloud service provider may be divided in to different levels, i.e. mail cloud service provider get data from data owner and share the data to the sub service provider in different levels without the knowledge of data owner. This may cause different security issues on data.



II. DATA SECURITY ISSUE ON CLOUD

- **Data location:-** When we use the cloud, we probably won't know exactly where our data is hosted. In fact, we might not even know what country it will be stored in.

- **Data Segregation**: - Data in the cloud is typically in a shared environment, data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists

- **Data at Data Centre:-**
  - Builds and maintains a secure data network
  - Protects cardholder data
  - Maintains a Vulnerability Management Programme
  - Implements strong access-control measures
  - Regularly monitors and tests networks
  - Maintains an Information Security Policy

- **Recovery: -** Even if we don't know where your data is, a cloud provider should tell us what will happen to our data and service in case of a disaster. Any offering that does not Replicate the data and application infrastructure across Multiple sites is vulnerable to a total failure.

- **Investigative Support:-**Investigating for illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

A. Data Classification:-

- Datas are classified based on its security not on its size and types.
- Public (Emp Name ,Designation ,Department)
- Sensitive (Emp Salary, Emp.Bank Balance)
- Restricted.

B. Security at Different Levels

We need security at following levels:

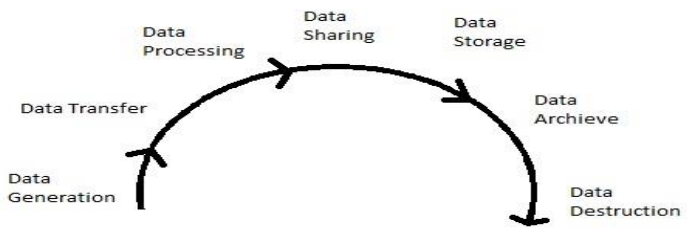
- Server access security
- Internet access security
- Database access security
- Data privacy security
- Program access security

C. Required Security Factors for Cloud Data:-

- RBAC (Role Based Access Controls)
- Trust Management with Service Provider.
- Data Backup
- Identity Management
- Authorization and Authentication

D. Data Management Life Cycle:-

Data life cycle refers to the entire process from generation to destruction of the data. The data life cycle is divided into seven stages. See the figure below



E. Data Generation

If data is to be migrated into cloud, it should be considered that how to maintain the data ownership.

F. Transfer

Within the enterprise boundaries, data transmission usually does not require encryption, or just have a simple data encryption measure. For data transmission across enterprise boundaries, both data confidentiality and integrity should be ensured in order to prevent data from being tapped and tampered with by unauthorized users. In other words, only the data encryption is not enough. Data integrity is also needed to be ensured. Therefore it should ensure that transport protocols provide both confidentiality and integrity.

G. Share

The data owners can authorize the data access to one party, and in turn the party can further share the data to another party without the consent of the data owners. Therefore, during data sharing, especially when shared with a third party, the data owners need to consider whether the third party continues to maintain the original protection measures and usage restrictions.
Regarding sharing of private data, in addition to authorization of data, sharing granularity (all the data or partial data) and data transformation are also need to be concerned about. The sharing granularity depends on the sharing policy and the division granularity of content. The data transformation refers to isolating sensitive information from the original data.

H. Storage :

The data in the cloud may be divided into:

- The data in IaaS environment, such as Amazon's Simple Storage Service;
- The data in PaaS or SaaS environment related to cloud based applications.

The data stored in the cloud storages is similar with the ones stored in other places and needs to consider three aspects of information security: confidentiality, integrity and availability. The common solution for data confidentiality is data encryption. In order to ensure the effective of encryption, there needs to consider the use of both encryption algorithm and key strength.
As the cloud computing environment involving large amounts of data transmission, storage and handling, there also needs to consider processing speed and computational efficiency of encrypting large amounts of data. In this case, for example, symmetric encryption algorithm is more suitable than asymmetric encryption algorithm.

Another key problem about data encryption is key management. Is who responsible for key management? Ideally, it's the data owners. But at present, because the users have not enough expertise to manage the keys, they usually entrust the key management to the cloud providers. As the cloud providers need to maintain keys for a large number of users, key management will become more complex and difficult. In addition to data confidentiality, there also needs to be concerned about data integrity.

When the users put several GB (or more) data into the cloud storage, they how to check the integrity of the data? As rapid elasticity feature of cloud computing resources, the users don't know where their data is being stored. To migrate out of or into the cloud storage will consume the user's network utilization (bandwidth) and an amount of time and some cloud providers, such as Amazon, will require users to pay transfer fees. How to directly verify the integrity of data in cloud storage without having to first download the data and then upload the data is a great challenge.

As the data is dynamic in cloud storage, the traditional Technologies to ensure data integrity may not be effective. In the traditional IT environment, the main threat of the data availability comes from external attacks. In the cloud, however, in addition to external attacks, there are several other areas that will threat the data availability:

- The availability of cloud computing services
- Whether the cloud providers would continue to operate in the future?
- Whether the cloud storage services provide backup?

I. Archival

Archiving for data focuses on the storage media, whether to provide off-site storage and storage duration. If the data is stored on portable media and then the media is out of control,
The data are likely to take the risk of leakage. If the cloud service providers do not provide off-site archiving, the Availability of the data will be threatened. Again, whether Storage duration is consistent with archival requirements?

Otherwise, this may result in the availability or privacy threats.

J. Destruction

When the data is no longer required, whether it has been completely destroyed? Due to the physical characteristics of storage medium, the data deleted may still exist and can be restored. This may result in inadvertently disclose of sensitive information. For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order to ensure no un-authorized access to organizations' cloud resources by some employees who has left the organizations. Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed.

III. CONCLUSION

Thus cloud computing also have various levels of security issues, where many companies are not interested in cloud due to lack of data confidentiality. Researchers need to give perfect solution for this security issues. Always cloud computing need to answer the following question to achieve higher level security measures.

- What kind of datas to be migrated in to cloud?
- How much Volume of data?
- How much security levels that data needs in reality?
- Making sure on higher level Authentication, Authorization, Access privileges, Confidentiality and Data consistency inside cloud.

References

[1] Vanya Diwan, Shubhra Malhotra, Rachna Jain, "Cloud Security Solutions: Comparison among Various Cryptographic Algorithms",IJARCSSE , April 2014.

[2] Gartner Inc, "Gartner identifies the Top 10 strategic technologies for 2011"

[3] David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez, "An analysis of securityissues for cloud computing Keiko Hashizume1". Science & Engineering Technology (IJCSET),2013.

[4] Cloud Computing Security Policies You Must Know ". Cloud Computing Sec. 2011.

[5] Gartner, "Seven cloud-computing security risks".

[6] Cloud Security Alliance. 2011, "Security Guidance for Critical Areas of Focus in Cloud Computing".

[7] Cloud Security Front and Center". Forrester Research. 2009-11-18.

[8] Hashizume , "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013.

[9] Rashmi, "A Survey of Cryptographic Algorithms for Cloud Computing". International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS),2013.

[10] EloffM.M, Smith E., "The management of security in Cloud computing", Univ. of South Africa, Pretoria, South Africa,2013.

[11] Maulik P. Chaudhari and Sanjay R. Patel, "A Survey on Cryptography Algorithms", IJARCSMS, 2014.

[12] Yu, Jiadi, Peng Lu, Yanmin Zhu, Guangtao Xue, and Minglu Li. "To-wards Secure Multi-Keyword Top-k Retrieval over Encrypted Cloud Data," IEEE transactions on dependable and secure computing, vol. 10, no. 4, pp. 239- 250, July/August 2013.

[13] Song, Dawn, Elaine Shi, Ian Fischer, and Umesh Shankar. "Cloud data protection for the masses", In IEEE Computer, vol. 45, no. 1, pp. 39-45, 2012.

[14] Swathi Sambangi "Cloud Data Storage Services Considering Public Audit for Security", Global Journal of Computer Science and Tech-nology Cloud and Distributed, ISSN: 0975-4172, Vol. 13, Issue 1, pp. 1 – 6, 2013.

[15] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Audita-bility and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[16] Srinivas, D. "Privacy-Preserving Public Auditing In Cloud Storage Security." International Journal of computer science and Information Technologies, ISSN: 0975-9646, vol. 2, no. 6, pp.2691-2693, 011.

[17] Zhu, Yan, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, and Stephen S. Yau. "Efficient provable data possession for hybrid clouds." In Proceedings of the 17th ACM conference on Computer and communications security, pp. 756-758. ACM, 2010.

Authors Short Profile:

Kavirajan Balakrishnan has been working as Assistant Professor with Mary Matha College, located at Nallakarupanpatti, Periyakulam, Theni District. He has qualified MCA., ME (CSE)., MBA(PMP). He has 4+ years of Software IT MNC experience and 4+ years of teaching experience. He is very much dedicated in research and in his teaching field to provide quality education which is a graceful and grateful service for Indian Society. Presently he is doing his research on Cloud Computing, Cloud Data Security, Big Data Analytics and Big Data visualization.

www.ioirp.com