International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 1, Jan-Feb 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Review Paperof CloudData Storage Security Issues

Sunita Patil*, Supriya Bhosale**

(Department Of Information Technology, DYPCOEAmbi,Pune))

----------**********----------

Abstract:

Cloud computing delivers on request services to its clients. Data storage is among one of the main services delivered by cloud computing. Cloud facility provider crowds the data of data holder on their server and employer can use their data from these servers. As data, employer and servers are different characters, the example of data storage brings up many security tests. In this paper, we will discuss the different types of techniques that are used for secure data storage on cloud.

Keywords — **Confidentiality, Cloud computing, Intigrity. Data Privacy;**

----------**********----------

I. INTRODUCTION

Security and privacy views as maincomplication on cloud computing i.e. conserving confidentiality, integrity and availability of data. A simple solution is to encrypt the data before uploading it onto the cloud.This method confirms that the data are not visible to outside users and cloud managers but has the restriction that plain text based searching algorithm are not applicable.

Cloud computing has become increasingly vital due to many associated features such as availability of data at any time,small cost storage.Mobile devices can gather personal data from many sensors within a smaller period of time and device based data contains of valuable data from users. But, mobile access presents many difficulties such as access to desired data, duplication to make data easily available,security of data, and AI techniques for quick and actual access to data. There are five types of cloud storage as Personal Cloud Storage,Public Cloud Storage,Private Cloud Storage and Hybrid Cloud Storage.We can describe cloud storage as storage of the data online in the cloud.When storage of data on cloud, it looks as if the data is stored in a exact place with specific name.In this paper, we discuss the security errors in data storage and the mechanisms to overcome it.

II. SECURITY AND PRIVACY ISSUES IN DATA STORAGE

Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements. But since there is no common cloud computing security standard, there are additional challenges associated with this. Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits.

Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises. The same internal and external threats are present and require risk mitigation or risk acceptance. In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing and implementing security control in a privately owned cloud.

III. CLOUD SECURITY THREATS

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. Confidentiality

Cloud providers with huge data stores holding credit card details, sensitive government or intellectual property andpersonal information, will be subjected to attacks from clusters, with significant resources, attempting to recover data. This contains the threat of hardware attack, social engineering and source chain attacks by dedicated attackers. For confirming confidentiality, cryptographic encryption algorithms and robust authentication mechanisms can be used. Encryption is the procedure of changing the data into a form named cipher text that can be understood only by authorized users. Encryption is an efficient method for protecting the data but have the problem that data will be vanished once the encryption key is closed.

B. Integrity

The integrity of data within composite cloud hosting environments such as SaaS configured to share computing resource betweenclients could provide a threat against data integrity if organization resources are effectively segregated.It is a technique for ensuring that the data is real, precise and protected from unauthorized users. As cloud computing supports resource allocation, there is a possibility of data being despoiled by unauthorized users

C. Availability

As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a risk that changes could present negative effects. These could be caused by software or hardware changes to present cloud services.

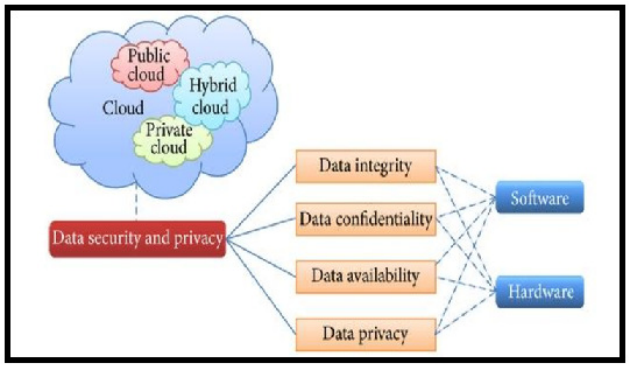

Fig.1Issues of Data Security and Privacy in Cloud Computing

D. Data Privacy

In the cloud, the privacy means when workers visit the sensitive data, the cloud services can prevent possible adversary from inferring the user's behaviour by the worker's visit model (not direct data leakage).

IV. CONCLUSIONS

Data security and privacy protection problems are applicable to both hardware and software in the cloud architecture. Cloud computing enables users to store their data in remote storage location. But data security is the major threat in cloud computing. Due to this many organizations are not willing to move into cloud environment. This study is to analysis different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and goals at enhancing the data security and privacy protection for the reliable cloud environment. In this paper, we make a relative research analysis of the existing research work regarding the data security and privacy protection methods used in the cloud computing.

.

REFERENCES

[1] A Venkatesh*1, Marrynal S Eastaff2 A Study of Data Storage Security Issues in Cloud Computing,8 IJSRCSEIT | Volume 3 | Issue 1..

[2] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, “Data Confidentiality and Integrity

Verification usingUser Authenticator scheme in cloud", Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India..

[3] Arjun Kumar, Byung Gook Lee, HoonJae Lee, AnuKumari, "Secure Storage and Access of Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "Highresolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[4] M.R.Tribhuwan, V.A.Bhuyar, ShabanaPirzade, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management", 2010 International Conference on Advances in Recent Technologies in Communication and Computing.(2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[5] Mr. Prashant Rewagad, Ms.YogitaPawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies.*FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[6] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Volume 3, Issue 1, January-February-2018 | www.ijsrcseit.com | UGC Approved Journal [Journal No : 64718] 1745 Distributed and Grid Computing (PDGC - 2010).A. Karnik, "Performance of TCP congestion control with rate feedback:TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute ofScience, Bangalore, India, Jan. 1999.

