Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Storage Security in Cloud Computing: A survey

Maulik Dave*
Department of Masters in Computer Engineering, LJIET
Gujarat Technological University,
Ahmadabad- India.

Abstract*— Cloud computing is the computing technology which provides resources like software, hardware, services over the internet. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. Cloud based data storage systems have many complexities regarding critical, confidential, sensitive data of client. The trust required on cloud storage is so far had been limited by users. The data storage in the cloud has been a promising issue in these days. This is due to the fact that the users are storing their valuable data and information in the cloud. The users should trust the cloud service providers to provide security for their data. The cloud service providers also providing the security but not up to a complete level. The attack of malicious insiders into the cloud and to steal the data has been increased. Data store is main future that cloud service provides to the companies to store huge amount of storage capacity. But still many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing. In this paper we have represented the survey on different issues related to data storage security on single cloud as well as multi cloud and fault tolerance.

Keywords*— Cloud; cloud computing; multiple cloud; service provider; data storage; data security; audit policy; data correctness; data availability; data integrity.

I. INTRODUCTION

Cloud computing is the next generation in the Internet's technology which provides the user everything in terms of services like computing power to computing infrastructure, applications, business processes as per the need of user over the internet. The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service [1]. Cloud computing has four main features: elasticity, self-service of provisioning and need base usage payment.

a. Deployment Models

There are Four different deployment models [2] of cloud computing.

1. *Public Cloud:*
   Public or external cloud is one of type of cloud in which user can use the recourses as per the need and pay for usage. This type of cloud also has various service providers who provide traditional cloud computing services to users and charged for it.
2. *Private Cloud:*
   Private cloud is the type of cloud in which the cloud is operated in only one organization or developed for one organization and managed by them or third party service provides. Basically this type of cloud is for the internal purpose of organization which is operated in geographically distributed.
3. *Hybrid Cloud:*
   Hybrid Cloud can be made up with the combination of two type of cloud like private and public cloud or the combination of cloud virtualization server with physical hardware. This type of cloud is much cost expensive compare to public cloud.
4. *Community Cloud:*
   If several organizations have similar kind of requirement, they can share the cloud then this type of cloud establishment is made possible in market. This cloud is also costly in compare to public cloud but provides high level security.

b. Cloud Computing:

Cloud computing is offered in different forms: public clouds, private clouds, and hybrid clouds, which combine both public and private [3].

1. *Cloud Software as a Service (SaaS) :*

Software as a Service provides software or application which can be used over the internet and user does not have not aware of any information regarding operating system, physical hardware. This type of application can be access via

internet and through browser at user side. User can have only some of control setting for application.

2. *Cloud Platform as a Service (PaaS) :*

Platform as a Service provide the setup of client's software packages and other tools which set up on service providers' physical hardware over the internet. So whole establishment is take place on service providers' environment and user can access that software after authentication process passes successfully. This user can free from the hardware failure problem by adopting this service.

3. *Cloud Infrastructure as a Service (IaaS) :*

In this type of cloud, user can have whole virtual server and user can access it as he can access it local like start, stop, and access and configure the server. In this type of service, user pays only for the capacity and model he needs them.

c. Benefits of Cloud Computing

1. Reduction in capital expenditure on hardware and software deployment.
2. Location independence, as long as there is access to the Internet.
3. Increased flexibility and market agility as the quick deployment model of cloud computing increases the ability to re-provision rapidly as required.
4. Allows the enterprise to focus on its core business.
5. Increased competitive advantage.
6. Increased security at a much lesser cost as compared to traditional standalone applications due to centralization of data and increased security-focused resources.
7. Easy to maintain as they don't have to be installed on each user's computer.

The cloud services that are implemented or those that will be implemented will always be accompanied by several threats. Knowledge about these threats shall prove to be the first step to prevent them. Hence security is the chief concern of several clients who desire to leverage cloud services. In all types of cloud, security issues arrive in many ways in different phases such as user's authentication, open source provision, virtual infrastructure, SLA, data storage and resource request[5]. Out of these, Cloud based data storage systems have many complexities regarding critical/confidential/sensitive data of client. The trust required on Cloud storage is so far had been limited by users [6]. The survey of related research work done on the cloud data storage security is discussed in the paper. The discussion spans the security challenges with respect to the type of deployment, service and common network issues.

II. RELATED WORK

In [6], Rakhi Bhardwaj et al. have represented dynamic data auditing policy for the data storage on the cloud. They have discussed on auditing model for the data storage in cloud which consists of data owner auditing, Third Party Auditing (TPA) and derived the resulting research where TPA can support the dynamic auditing for multiple tasks simultaneously. Thus, the high performance on data availability and integrity can be achieved. In [7], Yogita Gunjal et al. have presented new flexible and effective scheme for data integrity in terms of correctness for distributed storage system which removes or corrects code in the file distribution preparation to support redundancy parity vectors for verification of removed coded data using the homomorphic token .in cloud which consists of correctness insurance for storage integration, localization for data errors, data block dynamic operation. It gives efficient outputs against alternation attack and Byzantine failure. In [8], Gangolu Sreedevi et al. have presented new way of security ICCC for small organizations in cloud where data storage transparency can be minimized. They are not encrypting the whole message. Rather than encrypting whole message, they encrypt the some bits in each block. For data correctness, they have generated the Meta data which is used to verify the data for alteration or deletion by unauthenticated party. Through this technique, they achieve the correctness of data of owner at low cost and computational part is also free from overhead. In [9], Rupali Sachin Vairagade et al. have focus on the security of data in the cloud. Thus they have derived main three areas location of data, control of data and secure transfer of data in cloud, where data security is more concern. For security of the data, they have presented conversion of plaintext to ASCII Code and then the public key encryption RSA algorithm of ASCII code instead of plain text. So, only numeric data is to be encrypted instead of characters.

In [10], Kalpana Batra et al. have tried to achieve the security of data in distributed storage system by applying the file distribution technic to provide the redundancy. For correctness of the data they have generated the token pre computation technic and stored at servers in cloud for the verification purpose. They have shown that their scheme is efficient and reliable to detect the misbehaving servers and correct the data in particular servers and avoid colluding attacks of server modification by unauthorized users. In [11] K.RAJASEKAR et al. have proposed a secured cost-effective multi-cloud storage (SCMCS) model which consist of multiple cloud which provides the high availability and security compare to single cloud with economical cost to customer. Data is available among multiple SPs as per the budget of the customer. To ensure data availability, the user's data block is divided into various data pieces and distributed among the available SPs in such a way that no SP can make successful retrieval which have meaningful information. In [12], Qian Wang et al. have focus on the problem of simultaneous public audit of data and data dynamics on cloud storage for the integrity of data. They provide the solution which provides the efficiency for data dynamics by improving the storage models by manipulating the classic Merkle Hash Tree construction. They have used bilinear aggregate signature for the achieving their main goal of simultaneous multiple auditing task.

In [13], Mehdi Hojabri et al. have presented the effective and flexible data storage distribution method which handles the dynamic data with the authentication service which is provided by implementing the Kerberos authentication

service which include two main services authentication service and ticket granting service for authentication in cloud to provide the security in cloud. In [14], Amir Mohamed Talib et al. have ensured the confidentiality, correctness assurance, availability and integrity of users' data in the cloud by providing the Multi Agent Scheme (MAS) for the cloud storage which includes the different five type of agents Cloud Service Provider Agent (CSPA), Cloud Data Confidentiality Agent (CDConA), Cloud Data Correctness Agent (CDCorA), Cloud Data Availability Agent (CDAA) and Cloud Data Integrity Agent (CDIA) which distribute the work of data storage in cloud for better security as well as availability, correctness, confidentiality in the cloud. In [15], T.NEETHA et al. have proposed the model that will apply multi-clouds with secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. But, the interfaces between the cloud providers and the network traffic between the providers will still remain as a problem.

In [16], Anju Bala et al. have presented high availability of data and application by implementing the automatic fault tolerance technique for the application on cloud in which if one of the servers goes down, connection will automatically transfer to another server with data replication method and HAProxy. They have provide the availability of the application and data with replication technique with automatic fault tolerance

III. CONCLUSION

Although the usage of cloud computing has increased in market, but it has various security issues like data correctness, integrity, availability and etc. Owner of the data do not want to be stolen his data or data loss in cloud. Thus, high security and data availability must be maintained with in cloud. The main purpose of this work is to survey the recent research done on single cloud as well as on multi cloud to solve the security issues faced by the data owners. By this survey I conclude that much research has been done to address the security issue in data storage in cloud but for multi cloud that much of research is not done and still it has some security issues like data integrity and correctness at the time of data retrieval in cloud. So, multi cloud data storage security needs more attention in area of data storage security in cloud computing.

REFERENCES

[1] Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Fern Halper,"what is Cloud Computing For Dummies", "http://www.dummies.com/how-to/content/what-is-cloud-computing.html", last modified 2013.
[2] Jason, "Defining Cloud Deployment Models":" http://bizcloudnetwork.com/defining-cloud-deployment-models", Last modified on AUGUST 4, 2010.
[3] Margaret Rouse, "CLOUD APPLICATION PERFORMANCE MANAGEMENT: DOING THE JOB RIGHT", last modified December 2010.
[4] Anju Bala, Inderveer Chana, "Fault Tolerance- Challenges, Techniques and Implementation in Cloud Computing", in the year of January 2012.
[5] R. Yogamangalam and V.S. Shankar Sriram, "A Review on Security Issues in Cloud Computing", in the year of 2013.
[6] Rakhi Bhardwaj, Vikas Maral, "Dynamic Data Storage Auditing Services in Cloud Computing", in the year of April 2013.
[7] Yogita Gunjal, Prof. J.Rethna Virjil Jeny, "Data Security and Integrity of Cloud Storage in Cloud Computing", in the year of April 2013.
[8] Gangolu Sreedevi, Prof. C. Rajendra," ICCC: Information Correctness to the Customers in Cloud Data Storage", in the year of June 2012.
[9] Rupali Sachin Vairagade, Nitin Ashokrao Vairagade ," Cloud Computing Data Storage and Security Enhancement", in the year of August 2012.
[10] Kalpana Batra, Ch. Sunitha, Sushil Kumar," An Effective Data Storage Security Scheme for Cloud Computing", in the year of June 2013.
[11] K.Rajasekar & C. Kamalanathan," TOWARDS OF SECURED COST-EFFECTIVE MULTI-CLOUD STORAGE IN CLOUD COMPUTING", in the year of 2012.
[12] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing".
[13] Mehdi Hojabri," Ensuring data storage security in cloud computing with effect of Kerberos",in the year of July 2012.
[14] Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah, Masrah Azrifah Azmi Murad," Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi-Agent System Architecture", in the year of 2012.
[15] T.NEETHA, CH.SUSHMA," Security for Effective Data Storage in Multi Clouds", in the year of 2013.
[16] Anju Bala, Inderveer Chana," Fault Tolerance- Challenges, Techniques and Implementation in Cloud Computing",in the year of January 2012.

