A SURVEY ON RECENT TRENDS IN CLOUD STORAGE SECURITY

K. SAI VIJAYA LAKSHMI
Assistant Professor
Department of CSE,
GITAM School of Technology
vijayakommanaboyina@gmail.com

B. RAJENDRA PRASAD
Assistant Professor
Department of CSE, Sreenidhi Institute of Science and Technology
rajendranayakpb@gmail.com

ABSTRACT
Cloud computing is an emerging technology in the corporate world which enables the user to access the on-line resources like storage systems, servers, software and databases. These services are attracting the corporate companies to move towards the cloud technologies for better utilization of services. Cloud computing offers the user to utilize these resources based on their requirement over the inter-net. It provides the services like pay as per use policy. Though it provides exciting features to the user but maintaining the security for the cloud storage became a challenge to the service provider. The objective of this paper is to discuss about various issues related to the cloud storage, cloud storage security threats and the counter measures for the cloud storage security.

Keywords: *Cloud computing, Security threats, Service provider, Storage systems, Data bases.*

I. INTRODUCTION

Cloud computing: Cloud computing is a drastic shift from the way of traditional business to on-line business. In the cloud computing environment, the user needs not to make any large amount of investment to utilize the on-line resources. The user has to pay the amount only for the usage basis. Cloud storage is a model in cloud computing which offers the user to store, manage, manipulate and share the data remotely over the inter-net. In view of the salient features such as low cost investment, resource sharing, elasticity, quality of service and on demand services, etc.. cloud computing became very popular.

Cloud Deployment Models: The data owner has to select the required cloud deployment model which will be the major decision in cloud computing. Cloud deployment models are of into 3 types.

Private Cloud: Private cloud is designed exclusively for a single organization. Private clouds are appropriate for users who need customization and more control over the data. In private clouds security level is high and maintenance is easy. Private cloud examples are like Open stack, VMware etc..

Public Cloud: Public clouds are governed by the third party organizations. Public clouds are extensively used for unstructured data and it provides multi tenant storage. Here the cloud users access the cloud service through web browsers. This public cloud is based on pay-per-use criteria. By this, the cloud user can minimize the capital investment cost. It is less secure when compared to private cloud. [2]Public cloud examples are like Amazon web services, Google Docs etc..

Hybrid Cloud: Hybrid cloud is a combination of at least one public and one private cloud. By making use of Hybrid cloud, an organization can store actively used and structured data in private cloud, archival and unstructured data in public cloud.[1]

Service Models: Cloud service models mainly of 3 types

a. IaaS: Infrastructure as a Service is the lower level of the system. Infrastructure as a Service helps companies or organizations to migrate their physical infrastructure to cloud. The control of data over the

Infrastructure as a Service is similar to that of traditional infrastructure. It mainly reduces the capital or initial investment of buying servers. [3,4]IaaS follows pay-as-you-go policy. Consumers have the choice of selecting the entire server package like CPU configuration, bandwidth etc,..

b. PaaS: Platform as a Service is middle layer of the system. PaaS provides a developing environment as a service. It provides a tools and services for coding and developing new applications quickly and efficiently. It provides a platform for innovators for developing and testing new applications. The characteristics of PaaS includes a single platform for creating, coding, running and testing the applications.[5,6]

c. SaaS: Software as a Service is the upper layer of the system. SaaS is also known as On-Demand service [1]. SaaS provides software as a service for developers or companies. Here the applications are run on the cloud. This Software as a Service can accessed through web browsers or mobile applications.

Cloud Storage: Cloud Storage is the storage of digital data where a user or an organization can store the data and retrieves the data. The responsibility of keeping the data available, accessible, and protect from threats is done by the cloud service providers. Cloud storage offers unlimited storage of data. Users can use the storage space from service providers as per pay per use criteria. With the use of cloud storage, data is stored in multiple third party servers but not like in our traditional storage system.

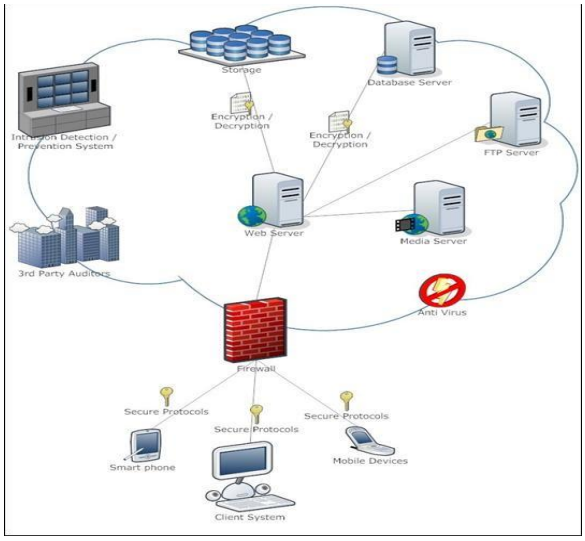

Figure Error! No sequence specified.:

Cloud Computing Environment

II CLOUD STORAGE SECURITY THREATS

Cloud Computing is the latest trend in the field of IT. It reduces the establishing costs for enterprises. Although Cloud Service Providers provide the excellent service, there are still some threats for cloud computing. They are

1. Data owner side: There may be chance of getting threats from data owner side those are

A. Software Vulnerabilities: Technology is emerging vastly for every decade use of computers, mobiles and other electronic devices has drastically increased over past 20 years. Internet has become vital element in one's life. Many of the tasks like inter-net banking, on-line shopping, and bill payments are done through inter-net. It made man's life easy, but on the other hand inter-net is highly vulnerable to various security attacks. Despite tremendous security services and mechanisms hackers still exploit the software vulnerability. Malicious users take this vulnerability as granted to cause various security issues which may reduce system information assurance.

B. Application Program Interface Threats: Some API's are accessible from anywhere on the inter-net. So, these API's become easy targets for malicious attackers. IT companies that provide cloud services allow the third parties to modify the API's and introduce their own functionality which in turn allow the companies to understand the inner working of the cloud. By understanding this, an attacker can get a token used by the customer to access the service through service API [8]. Attacker uses the same token to manipulate the customer data. Therefore API's became the major threat.

C. Web Browser Threats: it is known fact that in the world of computer networking, a client requests data from the server and the server responds to the client request. This communication's privacy and authenticity is assured by SSL. SSL also facilitates third party intervention in a secure fashion i.e it ensures secure point-to point communication. Problem arises where any intermediate third party gets dodged by an intruder. the intruder may attempt to grab the information shared between the parties for illegitimate purpose by installing various sniffing tools.

2. Network Channel Threats:

A. Confidentiality: Now a day's data for an enterprise in very huge and widely distributed legacy systems dictated data presents only in the vicinity of the organization due to emerging distributed trends the data is decentralized at various locations but virtually centralized using clouds the data in these clouds is highly vulnerable to security attacks. to ensure the confidentiality various encryption and decryption algorithms are incorporated.

B. Integrity: data on the clouds is accessed by all the authorized users as well as unauthorized users despite security measures. any user can get hold of the cloud data from any place hence cloud data's integrity is questionable as all kinds of user can get view and edit privileges in such a shared environment the user in this scenario is forced to trust the cloud service providers regarding data integrity.

C. Availability: availability of user data is another critical issue to be concern while using cloud services user may lose his data at any point of time. Due to fault of either user or cloud service provider the unfortunate user control question for his data loss.

3. Cloud Service Provider:

A. Virtualization: Virtualization mechanism has the ability to operate many resources like network devices, servers and operating systems on a single physical machine. The main motto of virtualization technique is to make the computing as more economical, efficient and scalable. So, using this technique the user can reduce the investment cost as compared with traditional way of computing. Due to this virtualization the major problems are huge data loss i.e if any damage to the physical device the entire virtual devices will collapse, integrity issues.

B. Phishing: It is an illegitimate process where the attacker creates a cloned website of a genuine website and grabs essential details entered by the users. phishing is widely used in financial frauds for example, a user in the inter-net wants to do on-line shopping he may be initially browsing the genuine website but unfortunately he may navigate to phishing website when he has to make payments for the orders as soon as he enters the credit card details the phishing website stoles those details and use them to generate unauthorized effect [12].

C. Access Control: Access control is one of the security measure incorporated to

ensure data protection users view and edit privileges can be restricted. On the other hand the owner can also prohibit the cloud service provider to view and edit his data. Some data is visible only after payment option. So, authenticated users are only allowed to fetch such kind of data due to access control mechanism.

D. Multitenancy: Different corporate companies are sharing their data centers to satisfy their business needs. This sharing of data is possible through the multi tenant support. Using this support many clients are sharing the data to reduce the cost. Due this openness there may be chance of violating the integrity and confidentiality properties especially in the public cloud environment. [13]

COUNTER MEASURES FOR CLOUD STORAGE SECURITY:

A. Reliability: Communication link is established prior to data transfer this communication is highly susceptible to frequent failures a reliable communication assures quick recovery of link failures giving the user an illusion that data is reduced to him seamlessly. This is achieved by buffering. On the other hand the failure may lure intruders to cause unauthorized hence security measures to be taken.

B. Provider Infrastructure: infrastructures provided by cloud services like IAAS should be secure, robust and scalable. To accommodate various emerging user needs the infrastructure is highly vulnerable to system crash or any natural disasters. Infrastructure should be able to carry on the work even if any module fails or any new module is added it should provide services over a period of a decade or more.

C. Backup: Any negligence in cloud services may lead to data loss which is questionable frequent data backup schedule should be designed and incorporated in clouds to equip the user to fetch 3 to 4 decades of old data.

CONCLUSION

Cloud computing offers the benefits like scalability, availability, multi tenancy, virtualization, less initial investment to the user. Though it is providing these many benefits but it is surrounded with so many challenges. This paper focused on the threats to the cloud storage security also the counter measures to the cloud storage security. By following these counter measures we can protect the data from the threats.

REFERENCES

[1]. Gorelik, Eugene. Cloud computing models. Diss. Massachusetts Institute of Technology, 2013.

[2].Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." Information Security for South Africa (ISSA), 2010. IEEE, 2010.

[3]. Kavitha, K. "Study on Cloud Computing Model and its Benefits, Challenges."

[4]. Hashim, Ali S., and Marini Othman. "Cloud Computing Adoption by Universities: Concepts and Review."

[5]. Comparison of Cloud Computing Service Models: SaaS, PaaS, IaaS 1 Sumit Khurana, 2 Anmol Gaurav Verma 1,2 Dept. of CSE, Surya World, Punjab, India

[6].Kaur, Gurleen, Ranjit Kaur, and Sita Rani. "Cloud Computing-A new Trend in IT Era."

[7]. Rajasekar, Narendran Calluru, and Chris O. Imafidon. "Exploitation of Vulnerabilities in Cloud-Storage." Journal on Computing (JoC) 1.2 (2014).

[8]. Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[9]. Qaisar, Sara, and Kausar Fiaz Khawaja. "Cloud Computing: Network/Security Threats And Countermeasures" published on Interdisciplinary Journal Of Contemporary Research In Business on January 2012."

[10] Chou, Te-Shun. "Security threats on cloud computing vulnerabilities." International Journal of Computer Science & Information Technology 5.3 (2013): 79.

[11] Kumar, Rajender, and Manish Kumar. "A Survey of Software Vulnerability and Auditing Tools."

[12] Jesudoss, A., and N. Subramaniam. "A Survey on Authentication Attacks and Countermeasures in a Distributed Environment." IJCSE, vol 5.2 (2014).

[13] Aljahdali, H, Albatli, A, Garraghan, P et al. (3 more authors) (2014) Multi-tenancy in cloud computing. In: Proceedings of the 8th IEEE International Symposium on Service-Oriented System Engineering. 2014 IEEE 8th International Symposium on Service Oriented System Engineering (SOSE), 7-11 April 2014, Oxford, UK. IEEE , 344 - 351. ISBN 978-1-4799-2504-9