International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 6, June-2018

A TECHNIQUE TO DATA STORAGE ON CLOUD:A SURVEY ON ISSUES, SECURITY AND BACK-UP

Sana Tak

Asst. Prof., Computer Science Department,Kalinga University, Raipur.

Abstract: Cloud computing is said to be the next big thing in the world of computer after the internet.In cloudcomputing, data is generated in electronic form which is very large in amount. It provides the facility to store the data online. The use of cloud computing is increase in industry and academics from last few years. As the data is stored online and in distributed form there is necessity of data security and recovery services in the cloud to prevent any data loss. In this paper we discuss various types of security techniques to data on cloud. We also discuss the data back-up technique for cloud computing. This paper will help the readers and researchers to know about the cloud security issues related to cloud. This will help the user to know about their data storage on cloud.

Key Words: cloud computing, data security, data back-up, cloud storage.

1. INTRODUCTION

“Cloud computing is a model for enabling on-demand and convenient network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provide”, the definition of cloud computing provided by NIST. Cloud storage provides the online storage where data stored in form of virtualized pool that is usually hosted by third parties. Cloud computing becomes popular as it provides scalability, flexibility and availability of data. Cloud computing becomes popular as it provides scalability, flexibility and availability of data. Any organization can store their data on cloud so as to use by their shareholder. Cloud provides various services and facilities but still there are various issues related to it. There are security issues related to data storage. The data files regarding clients are stored in any hardware devices which can be lost due to hardware problem like if the system gets physically crashed or data gets corrupted then there is no other source to recover it.

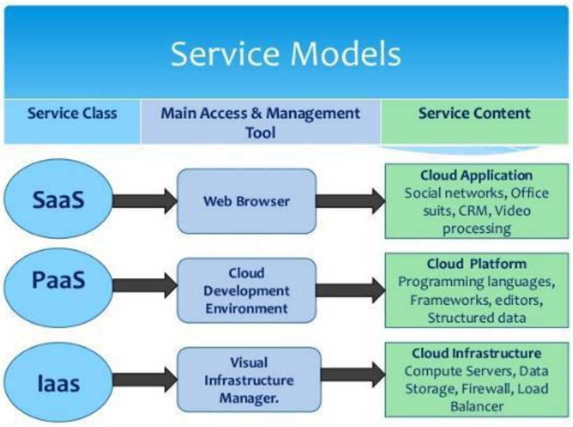
Service Models
Service Class
Main Access & Management Tool
Service Content
SaaS
Web Browser
Cloud Application
Social networks, Office suits, CRM, Video processing
PaaS
Cloud Development Environment
Cloud Platform
Programming languages, Frameworks, editors, Structured data
Iaas
Visual Infrastructure Manager.
Cloud Infrastructure
Compute Servers, Data Storage, Firewall, Load Balancer

Fig. 1 Cloud service model

In this paper we study various data security issues and attacks in cloud. We also analyze the techniques to secure the cloud model and data backup techniques..

2. ISSUES IN DATA SECURITY

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. Each service model is associated with some issues.

a) Multi-tenancy : It provides efficient utilization of resources, keeping cost lower. It implies sharing of computational resources, services storage and application with other tenants residing on same physical/logical platform at provider's premises. Thus it violates the confidentiality of data and results in leakage of information and encryption and increase the possibility of attacks.

b) Elasticity: It is defined as the degree to which a system is able to adapt to workload changes such that the available resources match the current demand at any time as closely as possible. Elasticity implies scalability. It says that consumers are able to scale up and down as needed. However this may lead to confidentiality issues.

c) Insider attacks: Cloud model is a multitenant based model that is under the provider's single management domain. This is a threat that arises within the organization. There are no hiring standards and providers for cloud employees [1]. So a third party vendor can easily hack the data of one organization and may corrupt or trade that data to other organization.

d) Outsider attacks: This is the one of the major issue in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network, they have more interfaces than private network. So hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking [1]

e) Data Loss: There are multiple tenants in cloud thus data integrity and safety could not be provided. Data loss can results in financial, customer count loss for an organization. An important example of this can be updating and deletion of data without having any backup of that data.

f) Network security:

- **I.** Man in middle attack:- In this attack, attacker establishes an independent connection and communicates with the cloud user on its private network where all control is in the hand of attacker.
- **II.** Distributed denial of service attacks: - In DDOS attack, servers and networks are overloaded with huge amount of network traffic and users are denied the access to a certain Internet based Service. [3]

3. TECHNIQUES TO SECURE DATA IN CLOUD

A. Authentication and Identity: Authentication of users is performed by various methods, but the most common is cryptography [8]. Authentication of users takes place in various ways like in the form of passwords that is known individually. One problem with using traditional identity approaches in a cloud environment is faced when the enterprise uses multiple cloud service providers (CSPs)[8]. In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution.

B. Data Encryption: If you are planning to store sensitive information on a large data store then you need to use data encryption techniques. Having passwords and firewalls is good, but people can bypass them to access your data. When data is encrypted it is in a form that cannot be read without an encryption key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key.

C. Information integrity and Privacy: Cloud computing provides information and resources to valid users. Resources can be accessed through web browsers and can also be accessed by malicious attackers [2]. A convenient solution to the problem of information integrity is to provide mutual trust between provider and user. Another solution can be providing proper authentication, authorization and accounting controls so the process of accessing information should go through various multi levels of checking to ensure authorized use of resources [2]

D. Availability of Information: Non availability of information or data is a major issue regarding cloud computing services. Service Level agreement is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and provider [2].A way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability.

E. Secure Information Management: It is a technique of information security for a collection of data into central repository. It is comprised of agents running on systems that are to be monitored and then sends information to a server that is called “Security Console”. The security console is managed by admin who is a human being who reviews the information and takes actions in response to any alerts.

F. Malware-injection attack solution: This solution creates a number of client virtual machines and stores all of them in a central storage.

G. Flooding Attack Solution: All the servers in cloud are considered as a fleet of servers. One fleet of server is considered for system type requests, one for memory management and last one for core computation related jobs. All the servers in fleet can communicate with one another. When one of the server is overloaded, a new server is brought and used in the place of that server and an another server that is called name server has all the record of current states of servers and will be used to update destinations and states.

4. TECHNIQUES FOR DATA BACK-UP IN CLOUD

This section explains all the data back- up and recovery techniques developed and used in Cloud Computing.
The Parity Cloud Service Technique is reliable, simple, easy and more efficient for recovery of data. It is based on parity recovery service. Using this method, data can be retrieved with a very high probability. The Parity information is created using the Exclusive-OR, though it cannot control the complexities generated while implementation [6].The laptop, smart phone users are handled by the HSDRT technique. It uses ultra-widely distributed data transfer mechanism along with high speed encryption. But the implementation cost is high and also redundancy cannot be controlled [7].The Efficient Routing Grounded on Taxonomy (ERGOT) Technique [8] is based on semantic analysis but has no focus on time and complexity of implementation. This approach helps for Discovery of Service in cloud computing. ERGOT provides an efficient way based on similarity of semantics to retrieve data. In Cold and Hot back up strategies, the cost of implementation increases as the data increases [9]. This approach performs recovery and backup based on the basis of failure detection. The services are triggered upon the detection of service failure in Cold Backup approach. The services won’t be triggered when available. In Hot Backup approach the services are in the activated state which is a transcendental strategy for service composition in dynamic network. These are the few techniques that are available for data back-up at remote cloud. The new techniques are also developing for data backup with more security.

5. CONCLUSION :

This paper describes some of the cloud concepts and its properties such as scalability, platform independent, low-cost, elasticity and reliability. Although there are various security challenges in cloud computing but in this paper, we have discussed some of them and also the techniques to prevent them, they can be used to maintain the secure communication and remove the security problems. This survey is basically done to study all the problems like attacks, data loss and unauthenticated access to data and also the methods for data back-up. In this paper we have discussed a few security approaches but several other approaches are also there that are in the process. Some standards are also specified which can be used to maintain secure communication and data storage at remote cloud and security in a cloud as many systems communicate in it and perform operations.

6. REFERENCES :

1. AkhilBehl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).
2. AkhilBehl&KanikaBehl (2012), An Analysis of Cloud Computing Security Issues.
3. L. Ertaul, S. Singhal& G. Saldamli, Security Challenges In Cloud computing.
4. Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009,
5. Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA(European Network and Information Security Agency), Crete, 2009.
6. Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, 2011, “Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service,” International Joint Conference of IEEE