RESEARCH ARTICLE OPEN ACCESS

Cloud Computing Security Single to Multi-cloud Using AES Algorithm

Miss.Kirti Sakhare, Miss.Swati Patil, Miss.Vijaya Shendage
Miss.Swati Kolhe

ABSTRACT

It has received cathedral (significant) attention in recent years but security issue is one of the major inhibitor in decreasing the growth of cloud computing. The client may not have any control and management of data. They are not fully authenticated, sometimes. The data stored and retrieved in such a way that they are Untrustiness i.e. the concept of TPA (Third Party Auditor) is used.TPA made task of user easy to verify integrity of data stored on represent of user. It provide Confidentiality, Integrity, Availability, Authenticity, and privacy. In this paper they are three delivery models such as Infrastructure as a Service (IaaS), PaaS (platform as a service), and SaaS (Software as a service) are present, they provide lot of security.

***Keywords*:-** Cloud Computing, Cloud, Security, cloud privacy, challenges, Third Party Auditor.

I. INTRODUCTION

The origin of the term is an intangible or cloudy. The term "cloud" is commonly used to since to represent a group of similar object (cluster). A cloud and describe any set of things whose details uninspected further in given contacts. The Cloud computing is an innovation (emerging) technology. It is an exaction (application) computing. It is an internet based computing that provide shared processing resources and data to computer and there devices application. It is module for enabling (pervasive) or Ubiquities exaction access to a shared pool of outline or structure computing resources. As earlier as possible it has drawn cathedral attention from both industry and colleagues. It provides services through the internet, by using cloud computing client. They can handle the online services of different software instead of translation them on their own systems terms. It is storage solution that provides user and enterprises with various capabilities to store and process there data in third party Auditor. Data security is one of the most important Specification or Parameter for client who want to use cloud computing. In cloud computing security can improve security focused on the resources etc. But here is a concerns can persist about loss control sensitive data and the lack of security are stored kernel side. Security obtain as good as or better than other classical systems, because of it providers are able to constant resources to solving security issues that many user cannot be able to goods. The complexity of security is rapidly increase when data is going from one to another throw the WLAN as well as in militant system shared by unrelated data. They must have industry in the marketing and Authenticate section. Now they are useful for digital Information Technology (IT) to store and process data. In this paper, we propose applying mathematical models as well as to develop a single cloud to multicolor as database cloud.

II. THEORETICAL BASELINE

Cloud computing is a network that user can use services provided by Service provider. A research environment provides a supreme range of applications of different topologies where each topology computing is expected to be adopted by government, manufacturers and academicians in near future. A communications and transmission of files over internet is increased since last few years, there is need of security for such file transfer. Solutions for secure communication are cryptography. It is converting plain text into encrypted text and decrypt cipher text to plain text at other end. There are two types of cryptographic algorithms: symmetric cryptography, asymmetric cryptography.

Cloud Computing Security Considerations

1. Cloud computing also offers potential benefits of cost savings and also improved business outcomes for Australian government agencies. There are a variety of information security risks that to be carefully considered. Risks will vary depending on the sensitivity of data to be stored or processed, and how the chosen as a cloud service provider has implemented their specific cloud services.

2. In this discussion of paper the assists agencies to perform a risk assessment is to determine the viability of using cloud computing services. The document provides an overview of the cloud computing it's benefits. This document provides a list of thought that are provoking questions to help agencies to understand the risks that need to be considered when using cloud computing. These are the questions in this document address the following topics:

a. For availability of data and business functionality of data;

b. The protecting data from unauthorized access,
c. and handling security incidents.

III. RELATED WORK

The paper, highlighted about that the customer could divide the data among several service providers (*SP*s).Also we provide a decision for the customer, for which *SP*s we must chose to access for data, with respect to the data access quality of service at the location of data retrieval. It was not only to rule out the possibility of a *SP* misusing of the customers' data, and the privacy of data, it also could easily ensure that data availability with a better quality of service. We introduced a method for quickly searching for the seed sets that scales to very large networks. In Our approach we found a set of nodes that guarantees spreading of the entire network under tipping model. From our point of view, number one service or feature that was missing is security of data. There were two levels of concern. One was focused on preventing others from reading the private data. It was a clear that concern and prominent in scenarios such as theft, and the other direct malicious attack. The other was concerned with the service provider reading of the private data. The two levels of concerns applied for other security issues as well, and of course were commensurate with level of confidentiality desired.

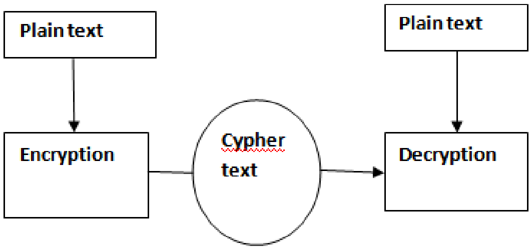


Figure 1. Symmetric Cryptography

IV. CLOUD COMPUTNG SERVICES

Service model of cloud computing

1)IaaS(Infrastructure as service):it refers to online services that abstract user for the detail of infrastructure like physical computing resources ,location ,data partitioning scaling ,security ,backup. IaaS cloud obtains offer additional resources such as virtual machines disk image library, raw block storage, file object storage, load balancer, ip address, and VLAN and software bundles. It provider supply this resources on demand large pool of equipment installed in data centre. The services are utilities computing basics.

2) PaaS (Platform as services):

It vendors offer develop environment to application developer. This provider typically develops toolkits standard for development and channel for distribution and payment. In PaaS model cloud provider deliver computing platforms, oeriting system, programming language, execution environment, and database and web server. Using that application developer can develop and there software solution on a cloud platform without cost and complexity of managing hardware and software layer. 1) Ex: it include iPaas and dPaaS. iPaas integrating platform as service and data platform as service.

3) SaaS: (Software as Service) in this model user gain access to application software and data base. it is a sometimes referred as on demand software and it usually prized on a paper per.basis.in this model cloud provider install and operate application software in the cloud and cloud users access the software for cloud client. The prizing model for SaaS Model is typically monthly or yearly plat properly user so price becomes adjacent and scalable. One drawback comes with storing the user data on the cloud provide server as a result there could be unauthorized access to data.

V. CLOUD COMPUTNG SECURITY ISSUES

The last few years, cloud computing has been grown from a promising business to the fastest growing segments of the IT industry. Recession-hit companies are increasingly realizing that simply by tapping into cloud they can gain fast access to the best-of-breed business of applications or drastically boost their infrastructure resources, at negligibly small cost. But more and more information on individuals and companies are placed in the clouds.

A. Security Issue

To see where your data is is more secure, on your local hard driver or on any high security servers at the cloud? Some argue that customer data is more secure when it is managed internally, while others argue for that, cloud providers have a strong incentive to maintain the trust of security. In the cloud, our data will be distributed over these individual computers of where our data is ultimately stored.

B. Privacy Issue

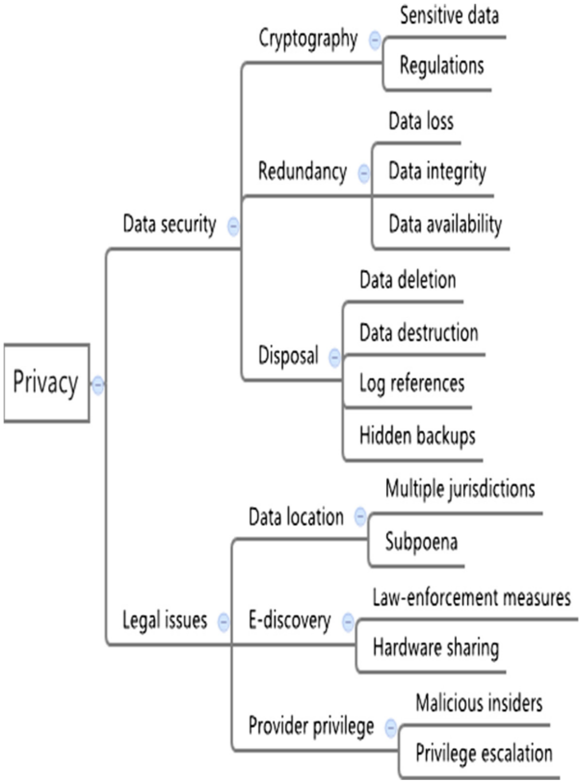
Cloud computing utilizes the virtual computing technology, for users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services.

C. Reliability Issue:

Servers in cloud have same problems as our own resident servers. Cloud servers experience downtimes, the difference are users have higher dependent on cloud service provider (CSP).

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, supplier such as Amazon Web Services provide a major market by developing restricted road and rail network “availability zones”



VI.TYPES OF CLOUDS

It is define type of access to the cloud that means how the cloud is located? Cloud can have any of the 4 type of access public private hybrid and community.

1) Public cloud: the public cloud allows systems and services to be easily accessible to the general public. Public cloud may b less secure because of its openness. Example: email

2) Private: the private cloud allows system and services to the accessible within an organization. it offers increased security because of its private of nature.

3) Community cloud: the community cloud allows system and service that can be accessible by group of organization.

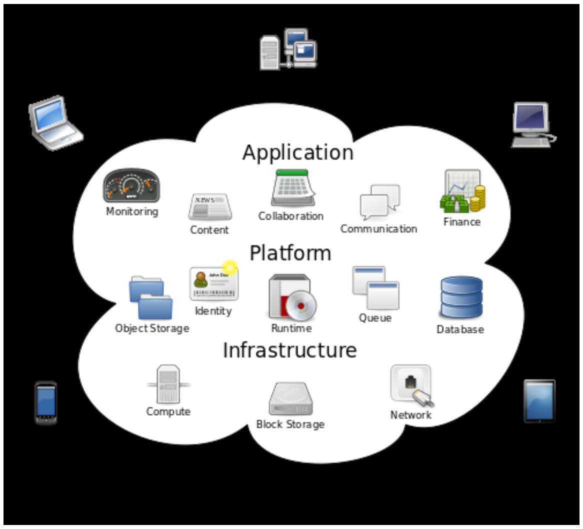
4) Hybrid cloud: The hybrid cloud is combination of public and private cloud. However the critical activities are performed using private cloud. While the noncritical activities are performed using public clouds

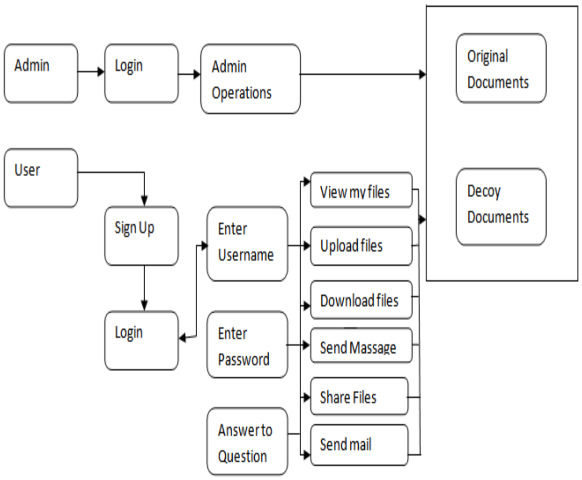
Attacks in a cloud computing environment

Types of attacks which are possible on clouds are.
User can be attacked by: Service SSL certificate spoofing, attacks on browser caches, or phishing attacks.
Cloud infrastructure: This attack that either originates at cloud spoofs to originate from the cloud infrastructure.
The service can be attacked: A user buffer overflow, SQL injection, and the privilege escalation are common types of attacks.
The cloud infrastructure can be attacked by: User targets the cloud control system.

VII. AECHITECTURE

The system architecture of software systems is used to deliver cloud services comprises hardware and software residing in the clouds. Physical location of infrastructure is determined by service provider as is the implementation of reliability and scalability logic of the underlying support framework. Virtual machines (VMs) are typically served as the abstract unit of deployment and are loosely coupled with cloud storage architecture. Applications are built on the programming interfaces of the Internet-accessible services and typically involve multiple intercommunicating cloud components.





VIII. CONCLUSION

In this paper we have explained different existing paper techniques and merits and demerits. We also discussed methods of the data security and privacy etc. In all papers some havent described proper data security mechanisms, and some were lack in supporting dynamic data operations, some were also lack in ensuring data integrity.

IX. REFERANCE

[1] J. Brodkin, Loss of Customer Data Spurs Closure of Online Storage Service Network World, August 11, 2008,

http://www.networkworld.com/news/2008/081108-linkupfailure. Html?page=1

[2] C. Brooks, Amazon EC2 Attack Prompts Customer Support Changes, October 12, 2009, http://searchcloudcomputing.techtarget.com/news/article/0,2 89142, sid201_gci1371090,00.html

[3] M. Calore, Ma.gnolia Suffers Major Data Loss, Magazine, January 30, 2009, http://www.wired.com/epicenter/2009/01/magnolia-suffer/

[4] D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition, January 2009, http://www.cert.org/archive/pdf/CSG-V3.pdf

[5] USA Patriot Act Comes under Fire in B.C. Report, CBC News, October 30, 2004, http://www.cbc.ca/canada/story/2004/10/29/patriotact_bc041 029.html

[6] R. Chow et al., Controlling Data in the Cloud: Outsourcing ACM Workshop on Cloud Computing Security, Chicago, IL, November 2009

[7] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, March 16, 2009, http://www.theregister.co.uk/2009/03/16/azure_cloud_crash/ Outage Hits Thousands of Businesses, CNET News, January 8,