International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 5, July - 2012

Assurance on Data Storage Security in Cloud Computing

HARIPRASAD AVULA
M.Tech(CSE)
MRCET,Hyderabad

G.RAVI
Assistant Professor
Department Of CSE

Abstract: *In the world of computing, resources utilization along with flexibility,scalability,robustness and security are the important issues as with cost and maintenance. For this we are having distributed computing, Gridcomputing, utility computing etc. these are facing difficulties any of the issue. For this a new era of computing technology come to picture with different services (Infrastructure as a service, Platform as a service, Software as a service)*[6] *called cloud computing. Cloud computing is pay perservice in real time via internet.*

It is a virtual world of computing so the machines and data storage maintain by the concerned parties,sometimes by third parties like outsourcing. So that the agreement between the user and service provider must be proper with legal support, it is called Service LevelAgreement (SLA). Here we are going to study a secured data storage structure that is moderated from traditional system.

Keywords: *Cloud data security, cloud computing Security issues, Cloud computing services, cloud data security issues*

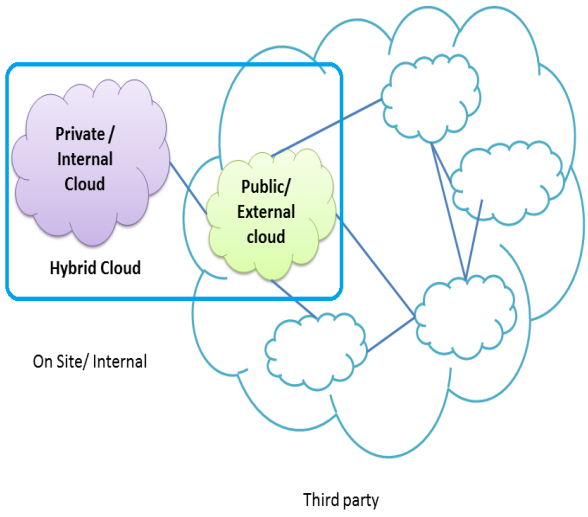
I. INTRODUCTION

In the traditional computing we need to purchase the infrastructure and the supporting software's related to work/project. The maintenance is also an overhead.
In the cloud computing everything is virtual to the user so that user will get the requirements with in low cost up to the required time. But in traditional it is not possible so that now a days cloud computing gets sound. It is not only useful for the small companies but also for big organizations. Think that a big organization/company got project related to simulators, so it needs infrastructure and maintenanceoverhead. For reducing this we go for cloud computing.

Cloud Services

As per the definition it must have the properties like feasibility, availability, scalability, reliability, reusability, sustainability, customizability and security [1].

Here we have three types of clouds, "Public Clouds" are mostly off premises , run by the third party companies(Google,Amazon,Microsoft etc.), "Private Cloud "are designed for an organization and maintenance also be done by that only, "Virtual private cloud " allow services to offer unique servicesto private cloud user[2].Sometimes we will call it as hybrid cloud.



Cloud Types

Cloud computing offers three types of services Infrastructure as a service (IAAS),Platform as a service (PAAS) and Software as a service (SAAS). Whatever the services provided by the service provider they are virtual so the user and service provider must be signed on SLA. It will be legal document/agreement, mostly it will depend on service providers country's cyber/IT law.

For the advantages of cloud computing it is getting popular. According to a recent Gartner survey[4] : Cloud computing services are estimated to account for 10.2 percentage of total spending on external IT services this year. Thirty-nine percentage of IT budget managers indicated that cloud computing is a key initiative for their organization.

Client
Application
Platform
Infrastructure
Server

Traditional computing environment

Forty-six percent plan to increase the use of cloud service. In another survey conducted by Gartner of CTO and CIos, over 76 percent of respondents fully expected that CRM(Client Relation Management) and productivity workload would be procured from the cloud.

II. Client Relation Management

Think that user needs Infrastructure as a service and Software as a service. So that these two services are integrated, and must be in touch with the user's requirement. The integrated thing will be called as Client Relation Management (CRM).

The Cloud services providers are clients to CRM(*ex: Microsoft Dynamic CRM online, soffront*) cloud and the user is an indirect client to the clouds under CRM, as a whole it is a cloud computing architecture.

CRM is an integrated suite of applications, can improve the customer experience by getting clouds to collaborateseamlessly [3]. It should support the adaptation of the different clouds, flexibility in user interface with drag and drop and promisebettercome end.

The document which defines the relationship between the service provider and client called SLA. It contains the information regarding the service definitions, performance management, problem management, customer duties and responsibilities, security,warranties and remedies, disaster recovery and business continuityand information about bills and dues [5].

Kandukuri, Paturi and Rakshit offer six recommendations for SLA content[5], including (1) special privilege user data access must be controlled to prevent unauthorized storage or retrieval, (2) cloud computing services must comply with relevant laws, (3) user data must be properly stored and encrypted, (4) a reset mechanism must be provided in case of service disruption or system crash, (5) service must be sustainable and guaranteed against service discontinuation due to change or dissolution of the provider and (6) if cloud computing services are used for illegal purposes, the provider must be able to provide records to assist with investigations.

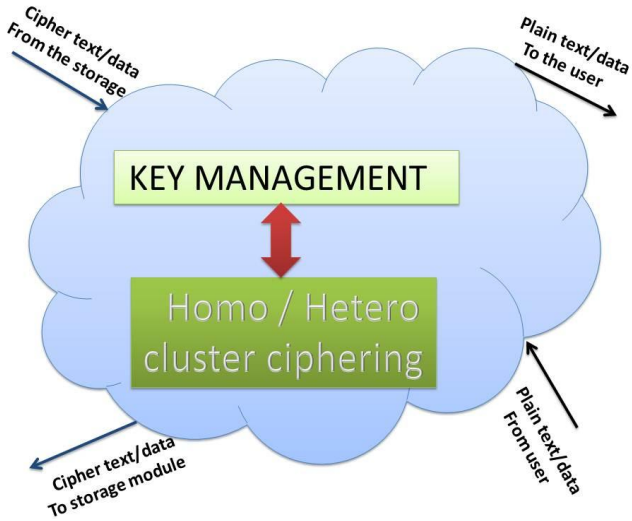
III.ASSURED DATA STORAGE SECURITY

The traditional storage system having the symmetric and asymmetric methods of encryption to provides security to data. These are the FIPS (Federal Information Processing System) AES (Advanced Encryption System) standard techniques with respective algorithms.

Here data storage and encryption done at storage service providers side. So the data and keys are available there, so it will cause privacy protection issue.

If we split the combinational (storage&security) service into two along with strengthen of security service it will avoid the issue.

Here we are using SSL[8] for secure data transmission and Cluster ciphering.Because SSL provides secured transmission channel in the network and it is used RSA algorithm for security. Here the work of the security service provider is to encrypt and decrypt the data and manage the keys. After encryption or decryption the data will be transfer to the data storage service or to the user on respective operations, the data present at security service providers will be deleted.



Studied Model for Data storage security

User will login to the cloud with the secured login mechanism(with OTP or with some secured mechanism).

When user wants to save the data he will send request to CRM, it will send the data to security service provider. Here after encryption the data will be transmitted to data storage cloud, after completion of storing it will send a response message to the user and acknowledgement to the security service cloud. On receiving the acknowledgement the encrypted data will be deleted.

In the data retrieving user will send a request to the data storage cloud through CRM. Data storage cloud will send encrypted data and the security service provider will decrypt the data and send it to the user.

In all process the communicative thing is CRM, so in case of maintenance, CRM provider should intimate users prior of five days at least.

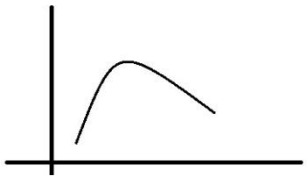
Here in this, the security provider should have the strong mechanism. As the advantage of cloud computing (Efficient use of resources) we are proposing cluster cipher technique.

It is nothing but using more than one cipher algorithm (Mechanism) to make the plain data as cipher data. Here we are having two types of Cluster ciphers.

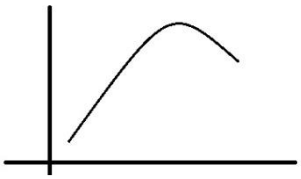
I. Homo cluster ciphering
II. Hetero cluster ciphering

Homo cluster ciphering means,using same class of ciphering mechanisms (synchronous or asynchronous) with different keys. The strength of cipher increased with number (N) of turns to be ciphered. The keys will be managed by the key management N(k)=(N{1,2,3…n}) module.

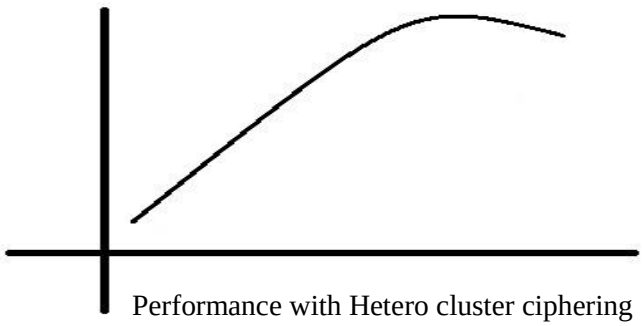
Hetero cluster ciphering means, using different class of ciphering mechanisms (combination of synchronous and asynchronous) with their respective keys. The key management as like Homo cluster ciphering but differs in the asynchronous key management like N(1, 2pub, 2pri, 3....n).



Performance with normal ciphering



Performance with Homo cluster ciphering



Performance with Hetero cluster ciphering

IVConclusion

As the advantages are concerned in this study, we are concentrating on the latest security policies, mechanisms and SLA with the reduction of management risks.

REFERENCES

[1] Malden A. Vouk"Cloud computing –Issues, Research and Implementations", JCIT-CIT 16, 2008, 4,235-246

[2] KapilBakshi"Cisco Cloud computing –datacenter strategy, Architecture, and Solutions", point of view white paper, 1st Edition.

[3] "Effective CRM solutions for small and medium size business" saffront.

[4]"Microsoft Dynamic CRM Online "Guide, version 1.o-JUNE 2011. Gartner1:1, 2011, Jones Lang LaSalle

[5]" Cloud Security Issues", Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.AtanuRakshit, 2009 IEEE International conference on service computing

[6] "A Break in the Clouds: Towards a Cloud Definition", Luis M.Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner- AC SIGCOMM computer communication Review , volume 39, Number 1, January 2009

[7] "RSA Algorithm",Pekka Riikonen,29.9.2002

[8] D.Wagner, B.Schneier, Analysis of the SSl 3.0 protocol, 2nd USENIX workshop on Electronic commerce, 1996.