ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Use of Cryptography and Secrete Sharing riven the Secrete into Multi-Cloud

Sanket Bora[1], Sandip Karale[2], Dheeraj Katariya[3], Ganesh Shejwal[4], P. P. Ahire[5]

UG students, Sinhgad Institute of Technology, Lonavala, Maharashtra, India[1,2,3,4]

Professor, Sinhgad Institute of Technology, Lonavala, Maharashtra, India[5]

Abstract: Cloud computing is one of the rising topic in the field of information technology. Now a day many organizations use this technology. There are many benefits of Cloud computing in terms of low cost and accessibility of Data. It is the smart technology and very popular, among all other computing paradigm. Security of cloud computing is a major factor in the cloud computing environment. Users store sensitive information with cloud storage providers but these providers may be untrusted. Due to risks of service availability failure and the possibility of malicious insiders in the single cloud Single Cloud is less popular. Security is one of the major factor that affect the growth as well as the development of cloud computing. This paper aims at the service availability of cloud. In this paper we give the solution for the cloud availability.

Keywords: Cloud computing, single cloud, multi-clouds, cloud storage, DepSky system, Shamir Secrete sharing algorithm, Data transfer security.

I. INTRODUCTION

Currently most of the organizations use the cloud computing to store own information of organization. When user deals with the single cloud provider there has problems such as service availability failure and the possibility that there are malicious insider in the single cloud. In recent days, customer has to move towards the multi-cloud. There are many security issues and challenges in cloud computing. In this paper we focuses on the data security of cloud computing. To protecting the data which has been stored by the users on cloud security plays an important role in that. Security plays an important role to the customers trust.

According to the National Institute of Science and Technology [NIST] cloud computing is a model for enabling convenient, on-demanding network access to a shared pool of configurable computing resources(i.e., network, server, storage, application, other services) that can be rapidly provisioned and released with minimal management effort or service provided interaction.

Cloud computing is classified into four deployment models, i.e. public, private, hybrid, and community. Public cloud is used in a public domain and private cloud is available for specific organization. The hybrid is combination of the different cloud deployment models, whereas the community cloud is for groups of organizations which take care of their agreement and privacy among the organization. There are three delivery models of cloud i.e. infrastructure as a service (IaaS), platform as service (PaaS), and Software as service (SaaS). IaaS, provides infrastructure, i.e servers, hardware, software and other supporting tools to fulfil. User do not need to buy the Infrastructure. In Paas, service providers provide the resources to the user on that user runs custom applications. In SaaS, user do not need to install software on their own machine. All required software are install and run on servers of cloud providers.

II. CLOUD COMPUTING SECURITY

Now days use of cloud computing has been increased very rapidly. Cloud computing refers manipulating, configuring, and accessing the applications online or decreasing the infrastructure costs [1]. Cloud computing security is most important issue for cloud service provider and users. To understand such aspect would help us to design a secure system in cloud computing. Cloud computing suffer from many issue related to its security such as data loss-leakage, shared technology venalities, insecure application interface, malicious insiders, abuse and nefarious use of cloud computing, account service and traffic hijacking. Since all the data is transferred over the internet, data security is major issue in cloud computing. Traditional security mechanism such as authentication, authorization is not only sufficient to cloud computing security.

A. SINGLE CLOUD IN CLOUD COMPUTING

Privacy protection and data integrity are the two main issues faced by single Cloud service providers. In his/her own organization one can ensure strong security policies. But in case of cloud computing one has to trust completely on his service provider [9]. Also there is an overhead of managing huge amount of data on a single server.

It is easier for malicious outsider to penetrate through security if the data is not actually stored by organization itself; instead they are trusting on third party for taking care of their data. Single Cloud computing require a High cost for cloud maintains process. And in single cloud computing Data has been loss in many times.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

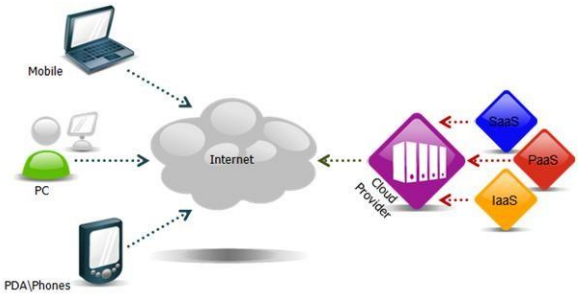

Fig 1: Single Cloud In Cloud Computing

Singlecloud can fail in ensuring the complete security from possible threats.

B. SECURITY RISKS IN SINGLE CLOUD

We have to add more security control to cloud computing so that client's sensitive data is secure and available all the time when needed. Cloud computing security is major aspect of data intrusion, Service availability and data integrity. To understand such security aspect is very helpful to design secure system in cloud computing. Following are security issues in single cloud or cloud computing.

1) ***DATA INTEGRITY:*** Data integrity is one of the most important issue in the cloud computing. Data stored in cloud computing may be loss or damage during the transition operation in the cloud storage provider. Data integrity in cloud computing security means data stored in cloud server only alter by only by authorized person. Computational integrity implies that the program is executed without being distorted by malware, cloud provider, or other malicious users and any incorrect computing will be detected [2].Data stored on the cloud is not modified and access by cloud service providers [3]. We have to add more security control to cloud computing so that client's sensitive data is secure and available all the time when needed. Cloud computing security is major aspect of data intrusion, Service availability and data integrity. To understand such security aspect is very helpful to design secure system in cloud computing. Following are security issues in single cloud or cloud computing.

2) ***SERVICE AVAILABILITY:*** Service availability means cloud service is available whenever user want his or her data i.e. cloud service available on demand. If user want to access his data but cloud server is down then there is huge loss of the user. In July 2008 due to some technical problem in Amazon cloud, the service of Amazon cloud is down for 6-8 hours [4].Now days Companies seek to protect their data and services from such failure they use of multiple Cloud service providers [5].

3) ***DATA INTRUSION AND SECURITY RISK:*** Data security is the most important aspect of the cloud computing security. Cloud computing have three service model Infrastructure as a service (Iaas), Platform as a service (Paas), Software as a service (Saas) [6].Cloud computing security involves the identification of threads and challenges and implementing the important step to provide the cloud security.

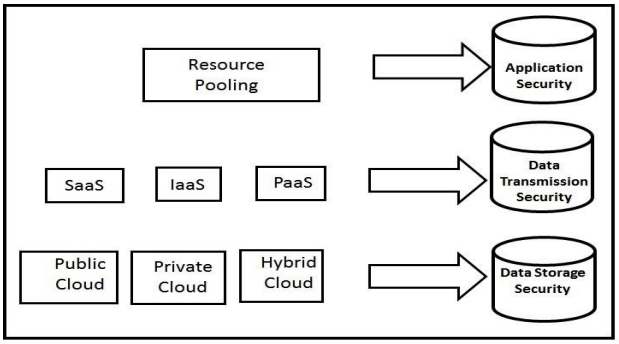

Fig 2: Security Pattern

Fig 2 shows the various security pattern with respect to the different cloud types, service models [7]. The CSA (Cloud Security Alliance) has identified. The Notorious Nine the top nine cloud computing threats for 2013[8].

1) Data breaches
2) Data loss
3) Service traffic hijacking
4) insecure interfaces and APIs
5) Denial of service
6) malicious insiders
7) cloud abuse
8) Shared technology vulnerabilities item Unknown risk profile.

Cloud users face security issues from both inside and outside the cloud.

III . MULTI-CLOUD SYSTEM IN CLOUD COMPUTING

In multi cloud data Storage, Data and Information will be shared with external users, therefore cloud computing users want to avoid important information from attackers or malicious insider is of critical importance.

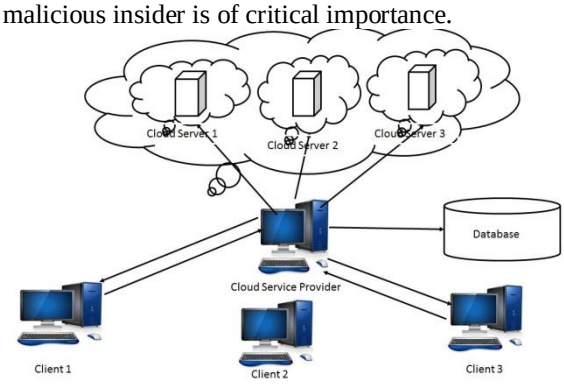

Fig 3:Multi-Cloud System

In Iaas, users are responsible for protecting operating system and cloud providers must provide protection for users Data Resources in the cloud are accessed through the Internet, frequently even if the cloud provider concentrates on security in the cloud infrastructure; the data is still

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

transmitted to the users through networks which may be insecure.

IV. PROPOSED SYSTEM

A. DEPENDABLE AND SECURE STORAGE IN A CLOUD- OF-CLOUDS (DepSky System)

In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behaviour and intrusion tolerance. Furthermore, many describe BFT as being of only purely academic interest for a cloud service [14].

In addition, it also includes arbitrary and crash faults [11]. This paper presents DepSky, a dependable and secure storage system that influences the benefits of cloud computing by using a combination of various commercial clouds to build a cloud-of-clouds. In other words, DepSky is a virtual storage cloud, which is accessed by its users by invoking operations in several individual clouds [12].

This system improves the availability, integrity and confidentiality of information stored in the cloud through the combining Byzantine quorum system protocols, encryption, secrete sharing and replication of the data on varied clouds that form a cloud-of-clouds. We deployed our system using four commercial clouds.

1) ***DATA MODEL:*** As the DepSky system deals with different cloud providers, the data format is accepted by each cloud, the DepSky library deals with different cloud interface providers and consequently.

The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

2) ***SYSTEM MODEL:*** The DepSky system model contains three parts: readers, writers, and four cloud storage providers Readers can fail arbitrarily whereas, writers only fail by crashing. For example, they can fail by crashing; they can fail from time to time and then display any behaviour.

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud.

B. REPLICATION OF ENCRYPTED DATA INTO MULTI CLOUD:-

If in case some data store in one cloud due to server down it can arise the problem of data availability in order to prevent this data(text ,image , etc.) has to be encrypted and each copy of encrypted data can be Stored in multi cloud. If user want to download the data from cloud and if in case the matches with the original key then decryption will take place. by means of which the user can retain its original data.

Simply replicate the data on multiple clouds solves the problem of data availability, but what about security. If there are multiple copies of the data, it will just open more doors for the gatecrasher to hack in.

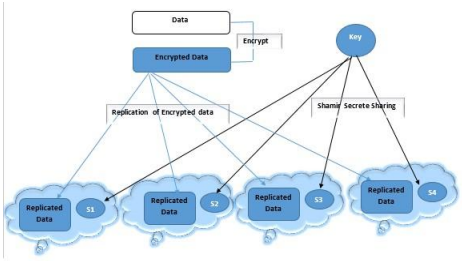

Fig 4:Replication of Encrypted Data into Multicloud

Thus there needs to be a way in which we can make sure that the data over multiple clouds is safe, or safer than it was in a single cloud. This is when we can apply the Secret sharing algorithm presented by, Adi Shamir elaborated in [10].

C. *SHAMIR SECRETE SHARING*

In cryptography, secret sharing refers to a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. We need secret sharing because Individual key share holder cannot change/access the data.

1) ***Mathematical Definition****:* Goal is to divide some data D (e.g the safe combination) into n pieces D1,D2,.Dn in such a way that: Knowledge of any k or more D pieces makes D easily computable. Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely). This scheme is called (k, n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.

2) ***Construction:***Construct n points (i,f(i)) where i=1,2..n Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S , which is the secret.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1}^{k-1}$$

3) ***Reconstruction:***In order to reconstruct the secret any 3 points will be enough

D. DATA TRANSFER SECURITY

The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients. The SSL data security transfer module establishes a SSL safe connection between the client terminal and the front end server of platform by SSL protocol in order to avoid interception, tamper and forgery by non-authorized clients in the process of data transfer [13].

V. CONCLUSION

Cloud computing security is still major issue in cloud computing because customer store it's secrete and important information on the cloud server so, it's cloud service providers responsibility to provide secure cloud storage. Data Intrusion, service availability and data

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

integrity are major aspect of single cloud security. In this paper we proposed secure and efficient multicloud architecture by using DepSky model, Shamir Secrete Sharing Algorithm and use of secure data transfer by using SSL. This Multi-Cloud architecture provide the very secure data transfer and storage on cloud server and also solve the major security problem in cloud computing security.

REFERENCES

[1] S. Subashini and V.Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (2011), pp-1-11.
[2] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing, Communication Survey & Tutorials", IEEE, vol.15, 2013, pp. 843-859.
[3] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS '07:Proceedings of the 14th ACM conference onComputer and communications security.
[4] Amazon, Amazon Web Services. Web services licensing agreement, October3, 2006.
[5] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.
[6] Peeyush Mathur, Nikhil Nishchal, "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
[7] E. B. FERNANDEZ 2013a. Security patterns in practice – Designing secure architectures using software patterns. Wiley Series on Software Design Patterns, 2013.
[8] Nine top threats to cloud computing security, http://www.infoworld.com/t/cloud-security, July 2013.
[9] Using Multi Shares for Ensuring Privacy in Database-asa-Service",44th Hawaii Intl Conf.on System Science (HICSS),2011,pp.1-9.M.A.AlZin and E.Parded.
[10] A.Shamir,"How to share a secret",Communication of the ACM,22(11),1979,pp.612-613
[11] M.Vukolic,"The Byzantine empire in the intercloud",ACM SIGACT News,41,2010,pp.105-111
[12] A.Bessani,M.Correia,B.Ouaresma,F.Andre and P.Sousa,"Depskay:dependable and secure storage in a cloud-of-clouds",EuroSys'11:Proc.6th Conf.on Computer System,2011,pp.31-46
[13] Xu Xiaoping ,Yan Junhu Research on cloud computing Security Platform ,2012 Forth International Conference on Computational and Information Science
[14] K.Birman,G.Chockler and R.van Reesse,"Toward a cloud computing research agenda",SIGACT News,40,2001,pp.68-80.

BIOGRAPHIES

Sanket Bora is student of BE in Information Technology from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in Information Technology in the year 2011 from S.H.H.J.B, Chandwad (Kd) in MSBTE.

Sandip Karale is student of BE in Information Technology from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University.

Dheeraj Katariya is student of BE in Information Technology from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University.

Ganesh Shejwal is student of BE in Information Technology from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in Information Technology in the year 2011 from Government Polytechnic Awasari (Kd) in MSBTE.

Mrs. P. P. Ahire (ME Computer Engineering) (Assistant Professor) Department of Information Technology, Sinhagad Institute of Technology, Lonavala.