Single to Multi Cloud Data Security in Cloud Computing

Hipparkar Pragati Damodar[1], Kadganchi Priyanka Vijay[2], Karche Sujata Vitthal[3], Prof. Shinde Ganesh Maruti[4]

[1,2,3,4]*Department of computer Science and Engineering, Shriram Institute of Engineering and Technology Centre, Paniv-Solapur, Maharashtra, India.*

---***---

Abstract *–Cloud computing is internet based. Resource sharing in a pure plug and play model that dramatically simplifies infrastructure planning is the promise of "cloud computing". The two key advantages of cloud computing are ease-of-use and cost-effectiveness. The cloud stores the large amount of data on single cloud as well as multi cloud. Here we implemented the single to multi cloud concept. Single cloud is less popular because is to risky of service availability failure and possibility of malicious insider single cloud. So the multi cloud concept becomes to increase cloud security. This paper aims to promote the use of multi cloud due to its ability to reduce security risks that affect the cloud users.*

Key Words: Security, Single cloud, Multi-cloud, AES, Secrete sharing, User, Admin.

1. INTRODUCTION

The internet is the interconnection of thousands of networks. The ARPANET began as a US Government experiment back in 1969. ARPA , the Department of Defence (DoD) advanced research project agency, initially linked researchers with a remote computer centers, allowing them to share hardware and software resources such as computer disk space, databases and computers. Later, this was shortened as —Internet. Cloud concept generated from the internet. There are different type of cloud services: SaaS, PaaS, IaaS. The underlying concept dates back to 1960 when John McCarthy opined that "computation may someday be organized as a public utility"; indeed it shares characteristics with service bureaus which date back to the 1960s. The term cloud had already come into commercial use in the early 1990s to refer to large ATM networks. By the turn of the 21st century, the term "cloud computing" had started to appear, although most of the focus at this time was on Software as a service (SaaS). While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Clod computing is computing paradigm, where large pool of system are connected in private or public networks, to provide dynamically scalable infrastructure for application data and file storage.

The proposed work considers data storage in Cloud Computing. Our contribution can be summarized as the following aspects:

1) The proposed work aims at data storage and efficient operations on data blocks.

2) The unauthorized users are prevented from accessing the data stored in cloud by using encryption and decryption and also the admin can block such users IP addresses. Client can't access and fetch resource which is stored in server until admin gives privilege to respective users.

2. Characteristics of Cloud

2.1 On-demand self-service: A user can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2.2 Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

2.3 Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

2.4 Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

2.5 Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

Layer	Cloud Computing Components
Five Characteristics	On Demand Self Services Broad Network Access Resource Pooling Rapid Elasticity Measured Services
Four Deployment Models	SaaS PaaS IaaS
Four Deployment Models	Public Private Community Hybrid

Fig. Cloud Environment Architecture

3. CLOUD SERVICES

3.1 SaaS – Software as a Service

A service provider delivers software and applications through the internet. SaaS is fundamentally the same as customer model of programming arrangement, where customers, for this situation as a rule internet browsers, give the purpose of access to programming running on servers. SaaS is the most well-known type of cloud administration for buyers. SaaS moves the assignment of overseeing programming and its organization to outsider administrations.

3.2 PaaS – Platform as a Service

Cloud Platform as a Service (PaaS), are utilized for applications, and other improvement, while giving cloud parts to programming. What designers gain with PaaS is a structure they can expand upon to create or alter applications. PaaS makes the advancement, testing, and sending of utilizations speedy, straightforward, and savvy. With this innovation, venture activities, or an outsider supplier, can oversee OSes, virtualization, servers, stockpiling, organizing, and the PaaS programming itself. Designers, in any case, deal with the applications.

3.3 IaaS – Infrastructure as a Service

Infrastructure as a service (IaaS)is a cloud computing offering in which a vendor provides users access to computing resources such as servers, storage and networking. IaaS services can be used for a variety of purposes, from hosting websites to analyzing big data. Clients can install and use whatever operating systems and tools they like on the infrastructure they get. Major IaaS providers include Amazon Web Services, Microsoft Azure, and Google Compute Engine.

4. TYPES OF CLOUD COMPUTING

4.1 Private Cloud

Private clouds are used for single user as well as small scale organization dealing with data protection and services level issue. It can access by only single user or authorized persons. Data access capacity of these cloud is limited. It is secure cloud based environment in which only the specified client can operate.

4.2 Public Cloud

Public cloud is used for big organization where number of user can access but it is not more secure as compare to private cloud. A public cloud is a type of computing in which a service provider makes resources available to the public via the internet. Resources vary by provider but may include storage capabilities, applications or virtual machines. Public cloud allows for scalability and resource sharing that would not otherwise be possible for a single organization to achieve.

4.3 Hybrid Cloud

Hybrid cloud is combination of private and public cloud. Hybrid cloud computing gives businesses the ability to seamlessly scale their on-premises infrastructure up to the public cloud to handle any overflow without giving third-party datacenters access to the entirety of their data.

5. MODULES

5.1 Admin Module

This module is responsible for authentication of client. User authentication is often the primary basis for access control. Authentication provides the access permission to only the authorized users and restricts the unauthorized users. This module also maintains data of user as like total login time.

5.2 Client Module

This module is responsible for UI Design of client .UI is designed by Jsp, Html, JavaScript, CSS, and JQuery etc. In this module, the client can send the query to the server for different requirement. Client module is also responsible for show retrieved in proper format means it also user friendly Design. It also responsible for client side validation for client pages.

6. ALGORITHMS

1. AES

The Advanced Encryption Standard (AES) is an encryption algorithm designed for securing electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is based on Rijndael cipher developed by cryptographers Joan Daemen and Vincent Rijmen. AES is currently available in three key sizes: 128, 192 and 256 bits. When migration of data to the chosen CSP happens and in future whenever an application uploads any data on cloud, the data will first encrypted using AES algorithm and then sent to provider. Once encrypted, data is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anywhere on cloud. This includes all types of data.

2. Secret sharing

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. The goal is to divide is secrets into piece of data D1,...,Dn Such way that:

1. Knowledge of any k or more Di piece makes S easily computable.

2. Knowledge of any k-1 or any fewer Di piece makes leaves S completely undetermined(in this all possible values are equally likely).This scheme is called as (k,n) threshold scheme. If k=n the all participants required to reconstruct secret.

7. CONCLUSION

The purpose of this work is to survey the recent research on single clouds and multi-clouds using. To securing data, encryption and secret sharing algorithms are the techniques used extensively to secure data. Also in this paper encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES algorithms to find the best one encryption algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers. Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, it has been found that AES algorithm uses least time to execute cloud data. DES algorithm consumes least encrypt-ion time. RSA consumes longest memory size and encryption time. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES

1. Cloud Computing Security: From Single to Multi-Clouds, 2012, 45th Hawaii International Conference on System Sciences.
2. Data Security In Cloud Computing, “International Journal of Science and Research” Volume 3 Issue 10, October 2014.
3. Data Security in Cloud “International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)”.
4. Data Secure in Cloud Computing Using Encryption Algorithms “International Journal of Science and Research”, Volume 4 Issue 3, March 2015.
5. Data Security and Authentication in Hybrid Cloud Computing Model ” 2012 IEEE Global High Tech Congress on Electronics”
6. Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.
7. Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (Cloud Com), IEEE Second International Conference 2010, On page(s): 693-702.
8. Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.
9. Gaidhankar Sushil, Kanase Amit, Lonkar Tushar, Patil Chetan "Multi-Cloud Storage Using Shamir’s Secret Sharing Algorithm ", Volume 1 issue 7,December 2014.
10. J. Archer, A. Boehm, “Security Guidance for Critical Areas of Focus in Cloud Computing”, Cloud Security Alliance, December 2009.
11. Seema L. Vandure , Jevi V. Gudaganavar “Security and data privacy in clouds”,2010

BIOGRAPHIES

Ms. Pragati Damodar Hipparkar is currently pursuing B.E (computer) from Dept. of Computer Science and Engineering, Shriram Institute Of Engineering and Technology Centre, Paniv, Maharashtra, India. She has received Diploma (Computer Tech.)Sahakar Marashe Shankarro Mohite Patil Institute Of Technology Research Shankarnagar Akluj. Her area of interest is Network Security, Developing.

Ms. Priyanka Vijay Kadganchi is currently pursuing B.E (computer) from Dept. of Computer Science and Engineering, Shriram Institute Of Engineering and Technology Centre, Paniv, Maharashtra, India. She has received Diploma (Computer Tech.) from Shriram Institute Of Engineering and Technology (Poly.), Paniv. Her area of interest Is Network Security.

Ms. Sujata Vitthal Karche is currently pursuing B.E (computer) from Dept. of Computer Science and Engineering, Shriram Institute Of Engineering and Technology Centre, Paniv, Maharashtra, India. Her area of interest Is Network Security.

Prof. Ganesh Maruti Shinde is currently working HOD of CSE Department at Shriram Institute of Engineering and Technology Centre, Paniv, Maharashtra, India. He has received M.E(IT) from DKGOI FOE, Daund. B.E (computer) from Dept. of Computer Science and Engineering from SB patil CoE Indapur. Maharashtra, India. Her area of interest Is Network Security and Operating 6 year Experience of professor).