ISSN: 2278 – 1323
*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 1, Issue 6, August 2012*

# Cloud Computing Data Storage and Security Enhancement

Rupali Sachin Vairagade[1], Nitin Ashokrao Vairagade [2]

***Abstract* - Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. We are in great need of encrypting the data. Our paper aims to give the cloud data storage methods and data security in cloud computing system. Here we propose a method for providing data storage and securing data in cloud computing system using RSA algorithm. In this algorithm some important security services including key generation, encryption and decryption are provided in cloud computing system.**

***Index Terms*—Data Storage, Security, Data Encryption, Data Decryption and Computation.**

## I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources.

Cloud is a new business model rapped around new technologies such as server virtualization that take advantage of economies of scale and multi-tenancy to reduce the cost of using information technology resources.

It also brings new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data.

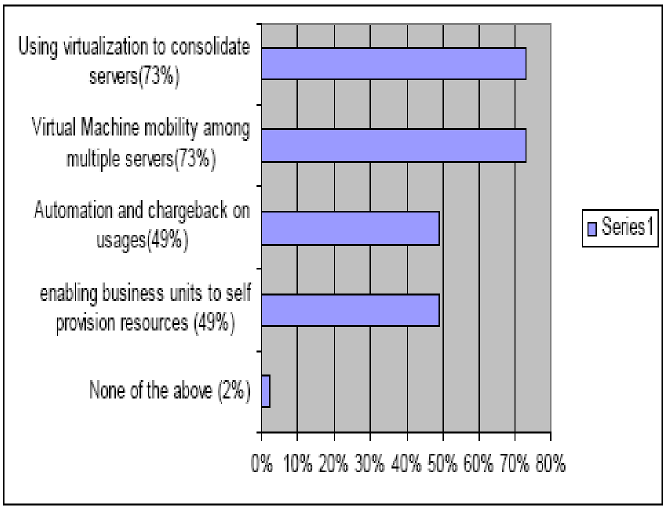

Fig.1 Technologies in cloud Environment.

Developers had asked IT professionals to tell what technologies they were currently deploying that support a current or planned cloud environment. Nearly three in four are currently using virtualization to consolidate servers and enabling virtual machine (VM) mobility across multiple servers (73 percent) in order to support a cloud. Nearly half offer automation and metering and chargeback based on usage and enable business units to self-provision resources.[6,7]

The advantage of cloud is cost savings. The prime disadvantage is security. Since the security is not provided in cloud, many companies adopt their unique security structure. For e.g. Amazon has its own security structure. Since the data placed in the cloud is accessible to everyone, security is not guarantee.

I propose a method for Cloud Computing system by providing data storage and securing Cloud Computing system using RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system.

## II. CLOUD STORAGE ARCHITECTURE

High-level architecture description of cloud data storage services illustrated in Fig. 2. The architecture consists of four different entities: *data owner*, *user*, *cloud server* (CS), and *Third party Auditor* (*TPA*).

Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. Under the cloud paradigm, the data owner may represent either the individual or the enterprise customer, who relies on the cloud server for remote data storage and maintenance, and thus is relieved of the burden of building and maintaining local storage infrastructure.

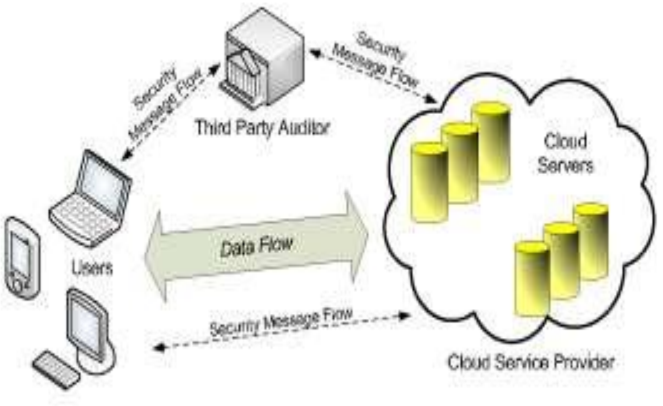

Fig. 2 Architecture of cloud computing

In most cases cloud data storage services also provide benefits like availability (being able to access data from anywhere), relative low cost (paying as a function of need), and on demand sharing among a group of trusted users, such as

All Rights Reserved © 2012 IJARCET

partners in a collaboration team or employees in the enterprise organization.[1,2]

## III. CHARACTERISTICS

| Characteristic | Description |
|---|---|
| Manageability | The ability to manage a system with minimal resources |
| Access method | Protocol through which cloud storage is exposed |
| Performance | Performance as measured by bandwidth and latency |
| Multi-tenancy | Support for multiple users (or tenants) |
| Scalability | Ability to scale to meet higher demands or load in a graceful manner |
| Data availability | Measure of a system's uptime. |
| Control | Ability to control a system in particular, to configure for cost, performance, or other characteristics. |
| Storage efficiency | Measure of how efficiently the raw storage is used. |
| Cost | Measure of the cost of the storage (commonly in dollars per gigabyte) |

## IV. CLOUD STORAGE MODELS

There are models for cloud storage that allow users to maintain control over their data. Cloud storage has evolved into three categories, one of which permits the merging of two categories for a cost-efficient and secure option. Public cloud storage providers, which present storage infrastructure as a leasable commodity (both in terms of long-term or short-term storage and the networking bandwidth used within the infrastructure). Private clouds use the concepts of public cloud storage but in a form that can be securely embedded within a user's firewall. Finally, hybrid cloud storage permits the two models to merge, allowing policies to define which data must be maintained privately and which can be secured within public clouds.

Examples of public cloud storage providers include Amazon and Nirvanix (which offer storage as a service), Private cloud storage providers include IBM, Para scale, and Clever safe (which build software and/or hardware for internal clouds) and hybrid cloud providers include Nirvanix and Egnyte, among others.

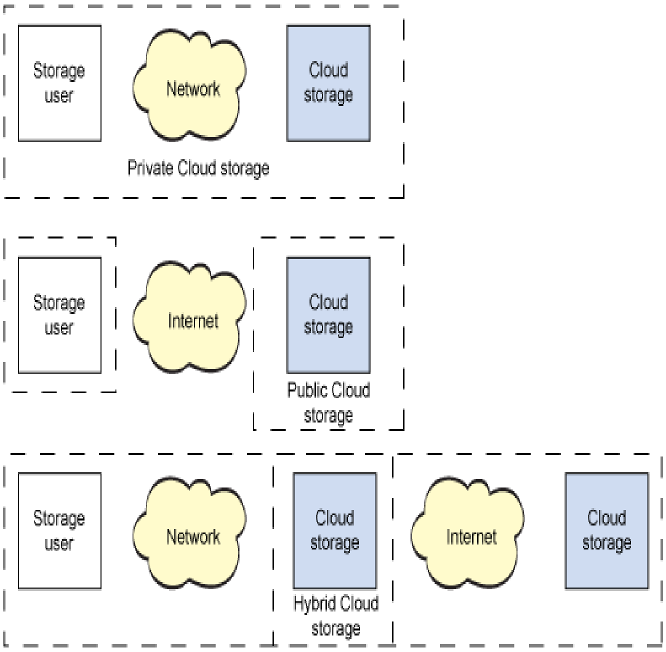

Fig.3. Cloud storage models

## V. SECURING DATA IN CLOUD

There are three key areas of concern related to security and privacy of data:

1. Location of your data
2. Control of your data
3. Secure transfer of your data

A. Data location in the cloud:

1. *Data transfer across country borders*: A global company with subsidiaries or partners (or clients for that matter) in other countries may be concerned about cross-border transfer of data due to local laws. Virtualization makes this an especially tough problem because the cloud provider might not know where the data is at any particular moment.

2. *Co-mingling of data:* Even if your data is in a country that has laws you're comfortable with, your data may be physically stored in a database along with data from other companies. This raises concerns about virus attacks or hackers trying to get at another company's data.

3. *Secondary data use:* In public cloud situations, your data or metadata may be vulnerable to alternative or secondary uses by the cloud service provider. Without proper controls or service level agreements, your data may be used for marketing purposes (and merged with data from other organizations for these alternative uses). The recent uproar about Face book mining data from its network is an example. The service provider may own any metadata has created to help manage your data, lessening your ability to maintain control over your data.

All Rights Reserved © 2012 IJARCET

B. Data Control in the Cloud :

Data controls include the governance policies set in place to make sure that your data can be trusted. The integrity, reliability, and confidentiality of your data must be beyond reproach. For example, assume that you're using a cloud service for word processing. The documents you create are stored with the cloud provider. These documents belong to your company and you expect to control access to those documents. No one should be able to get them without your permission, but perhaps a software bug lets other users access the documents. This privacy violation resulted from a malfunctioning access control**.** Here is a sampling of the different types of controls designed to ensure the completeness and accuracy of data input, output, and processing:

Input validation controls to ensure that all data input to any system or application are complete, accurate, and reasonable. Processing controls to ensure that data are processed completely and accurately in an application. File controls to make sure that data are manipulated accurately in any type of file (structured and unstructured). Output reconciliation controls to ensure that data can be reconciled from input to output. Access controls to ensure that only those who are authorized to access the data can do so. Sensitive data must also be protected in storage and transfer. [8]

C. Securing data for transport in the cloud*:*

A *virtual private network (VPN) is one way to manage the security of data* during its transport in a cloud environment. A VPN essentially makes the public network your own private network instead of using dedicated connectivity. Virtual private networks (VPNs) provide the ability to create a secure network connection across a public network through the use of encryption and Firewall.[8] It's necessary to note that the VPN itself has multiple implementations.

VPN types include network-to-network, multiple service host-server, to single-service host-server. Each of these implementations can be used in a cloud computing environment, and each has security strengths and weaknesses.[3]

*1. Network-to-network VPN:*

The oldest VPN technology is the network-to-network VPN. This architecture has the greatest risk associated with it, due in part to the number of hosts involved.

This model gives an attacker the ability to use many services on many hosts in order to gain access and control of cloud computing data. The network-to-network VPN provides network transparency and management that enables inspection of the traffic after the point of decryption, but it does not protect the data payload end-to-end. Once any portion of the cloud is compromised, all other portions connected to that cloud via network-to-network VPN technology must be considered compromised. This is worse than the old "reverse Darwinism" problem that occurs when a network with strong security controls is connected to a network with weaker controls, such as through a VPN tunnel and the more a secured network is exposed to vulnerabilities via the weaker one.

*2. Single-host-to-server VPN*

The second type of VPN is the single-host-to-server VPN, or point-to-point VPN. This VPN provides the encrypted tunnel from client to host for multiple services. Because this connection, much like the network-to-network connection, takes place at layer 3 (or lower), many of the same security issues found in the network-to-network VPN exist here. Fortunately, most cloud computing service providers elect to use the service-to-host model through SSH, SSL or another dedicated service.

The single service-to-host model is not without flaws. However, by limiting the size of the access area, the overall security footprint decreases, thereby making monitoring and securing it more manageable. The service-to-host model offers the opportunity to monitor the entire session. The cloud service provider has the ability to insert logging software, as well as security controls, into the processing. Naturally, the security controls and logging are dependent on the cloud computing service provider's security model. Since logging and event monitoring are required components of most organizations' compliance programs.

The use of single-service VPN access to the cloud is considered the most secure and can decrease vulnerability exposure to both the client and the server. However, the client must still remain aware of the cloud server(s) architecture and must extend as much of his security model into the cloud as possible.[11]

## VI. SECURITY IN CLOUD COMPUTING USING RSA

*1. RSA Definition:* Public key encryption algorithm has been developed by Rivest, Shamir, and Adleman in MIT as pioneers work. By taking their initial name, this algorithm is called RSA-encryption system.

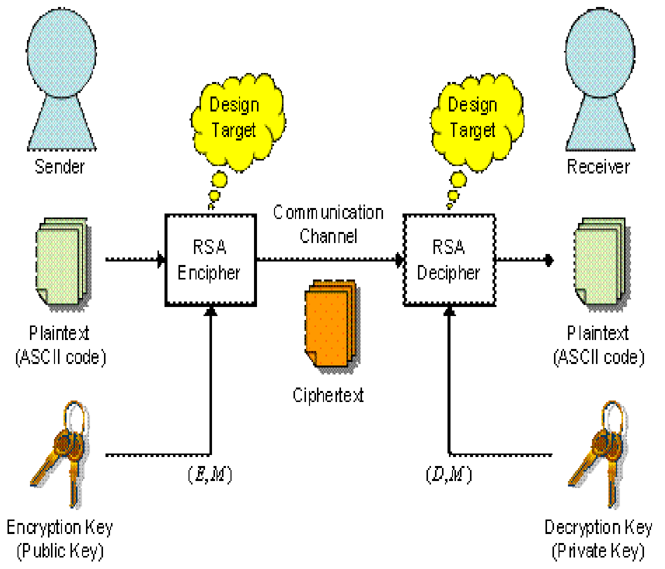

Fig. 4 Overview of RSA Algorithm

The RSA encryption algorithm is widely used such as for emails and files encryption system called PGP(Pretty Good Privacy),for e-commerce encryption system called SSL (Secure Socket Layer) and so on. In spite of widely used encryption algorithm, the RSA requires a lot of time for encryption and decryption of plane text. This is due to its heavy computational complexity since it makes use of prime factorization with respect to two prime number product.

## *2. RSA Encryption Algorithm in detail:*

Let us define some integer parameters P as a plain text, C as an encrypted text, E as the encryption key, D as the decryption key, and M as modulo number. The encryption can be made by following equation.

$$C = P^{E} \bmod M \qquad (1)$$

Where mod expresses a modular operation. On the other hand, the following equation is used for decryption

$$P = C^{D} \bmod M \qquad (2)$$

As we can see in Eq.(1) and (2), the RSA encryption system's expression itself is not complicated. At the first step how to define E, D and M. we randomly choose quite large number of two prime factors p and q ($p \neq q$). Then modulo M is defined as $M = p \times q$. From p and q, we define

$$L = \mathrm{LCM}(p-1, q-1) \qquad (3)$$

Where LCM stands for the least common multiple. The encryption key is chosen as a certain number which is less than and mutually prime with L. Therefore E can be expressed as

$$\mathrm{GCD}(L, E) = 1 \qquad (4)$$

Where GCD stands for the greatest common devisor. In order to shorten the processing time (computational complexity), E is often chosen to be relatively small number. Lastly, the decryption key D should satisfy the following equation for arbitrary integer number H.

$$E.D = H.\,L + 1 \qquad (5)$$

By using above defined E, D and M, encryption and decryption can be carried out according to the Eq.(1) and (2). See some references for more theoretical explanation. As you might already realize it, the decryption key D can be easily obtained if the modulo M can be prime factorized; however, as far as M is chosen as several hundred digits, prime factorization would take more than several to 10 years or more even by using a state-of-the-art super computers. This ensures the robustness against attacking in terms of the RSA algorithm.[10]

In this algorithm, n is known as the modulus, E is known as the encryption exponent, D is known as the secret exponent or decryption exponent.

## 3. *RSA Example:*

1. Key generation:

Suppose we choose P =11 and Q=23, find the encryption key E, the decryption key D, and modulo M.

$$M = P \times Q = 253$$

$$L = \mathrm{LCM}(11-1, 23-1) = 110$$

According to Eq. (4), E satisfies

$$\mathrm{GCD}(L, E) = 1$$

Therefore,
E=101 is one of the candidate.

If we choose H=56 as an arbitrary integer number, then D=61 according to Eq. (5)

2. Encryption and decryption:

Suppose we make use of the ASCII code, to convert Alphabet characters into certain integer numbers. Encrypt the following plain text into cipher text. Then decrypt this cipher text into the original plain text. Here we encrypt a plane text one character by one character. Normally, a block wise processing, which means several characters are encrypted as block manner, is used for it.

*Plain text:* Enjoy HDL!
According to ASCII code, we get

*Coded plain text:*

69 110 106 111 121 32 72 68 76 33

Applying Eq (1) into first character 'E', which is 69 in ASCII code, we get

$$C = P^{E} \bmod M$$

$$C = 69^{101} \bmod 253 = 69$$

This number 69 is the encrypted code in terms of the first character 'E'. The problem in this equation is that heavy complexity is required for power calculation. The solution of this problem could be one of the goals for better RTL design. As was same manner for the first character, the whole plain text can be encrypted as follows.

*Encrypted (Cipher) text:*

69 209 172 122 220 219 193 68 43 176

This cipher text can be decrypted by using Eq. (2). For the first encrypted data '69', we get

$$P = C^{D} \bmod M$$

$$P = 69^{61} \bmod 253 = 69$$

This is nothing but character 'E' as was in the original plain text. In this way we decrypt other cipher text all together.[9]

All Rights Reserved © 2012 IJARCET

## VII CONCLUSION

In this paper, we give the overview of data storage in cloud computing and the security in cloud system. Here the main idea is to give integrity to the cloud storage area with different data models and security algorithm.

We first present the cloud data storage architecture along with the cloud data models. Then we suggest the algorithm for cloud security using RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system. The main goal is to securely store and manage data that is not controlled by the owner of the data. The data are stored in cloud environment Cloud security here is solved by providing an RSA algorithm.

## REFERENCES

[1] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[2] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in , cloud Computing", 2010.

[3] Ramgovind S, Eloff MM, Smith E ,"The Management of Security in Cloud Computing", School of Computing, University of South Africa, Pretoria, South Africa ©2010

[4] Jianfeng Yang and Zhibin Chen ," Cloud Computing Research and Security Issues", IEEE 2010.

[5] S. Sajithabanu and Dr. E. George Prakash Raj, "Data Storage Security in Cloud" IJCST Vol. 2, Issue 4, Oct. - Dec. 2011.

[6] Sunita Rani and Ambrish Gangal, "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", (IJCSIT) ,Vol. 3 (3) , 2012,4302 – 4304.

[7] Alok Tripath and Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE.

[8] "Advance Computer Technology" a book by Dr. Deven shah. Edition-2011.

[9] "Cryptography and Network Security" a book by William Stallings, Fifth Edition

[10] http://www.lsi-contest.com/2008/spec2_e.html.

[11] http://searchcloudsecurity.techtarget.com/tip/Cloud-computing-security-Choosing-a-VPN-type-to-connect-to-the-cloud.

*First Author* :- PG,Student, Department of M.E Computer Engg.,Pune Institute of Computer Technology, Pune.
*Teaching Experience* :- Four year

*Second Author*:- Graduate student, Department of C.E. and I.T., St. Vincent pallotti College of Engg. and Tech.,Nagpur