Volume 5, No. 4, April 2014
Journal of Global Research in Computer Science
ISSN-2229-371X
Review Article
Available Online at www.jgrcs.info

SAVE AND SECURE DATA ON CLOUDS

Sonia Verma[1]* and Amit Kumar Chaudhary[2]
[1]*Student (CSE) , Asst. Professor(CSE) [2]
Swami Vivekananda Subharti University
Meerut, U.P., India
sonverma@gmail.com,Amitakg84@gmail.com

Abstract — The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data In the cloud environment, resources are shared among all of the servers, users and individuals. So it is difficult for the cloud provider to ensure file security. As a result it is very easy for an intruder to access, misuse and destroy the original form of data.. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted..A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. In this paper, we discuss security issues for cloud computing and how to secure the data over the network. So that user can build trusted applications from untrusted components will be a major aspect of secure cloud computing.

Index Terms — Cloud Computing, Security, RSA, Shamir Secret Sharing Algorithm.

I. INTRODUCTION

Cloud computing is an innovation of existing technology where cloud introduce the innovative and cost effective concept of services for both public and private sector. Cloud computing also introduce the resource sharing concept and secure the data also.

"Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer tointernal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing." (Armbrust et al., 2009, p6)

Features of cloud computing:

- Cloud computing is a new computing paradigm
- Cloud computing allow to share the resources(hardware and software)
- Clouds provide the virtualization
- Clouds are consumed either Web browser or defined API
- Data security is also an very important features.

Essential Characteristics of Cloud Computing

There are 7 essential characteristics of cloud computing.

1. Client can use or unused the service when needed, without any human interaction with service provider.
2. Service can accessed anywhere and anytime in the world over the world through some standard mechanisms.
3. Resource can be shared by the multiple user and pooled to serve multiple consumer.
4. Service can be rapidly and elastically provisioned.
5. Cloud Computing systems automatically control and optimize resource usage by providing a metering capability to the type of services (e.g. storage, processing, bandwidth, or active user accounts) .
6. Security of data is very important while accessing the data over the internet.
7. Reduce the cost of the data.

Cloud Deployment Models

- *Public Cloud*

The cloud infrastructure is available to the general public.

- *Private Cloud*

The type of the cloud, that is available solely for a single organization.

- *Community Cloud*

In this type of cloud deployment model, the infrastructure of the cloud is shared by several organizations and supports a specific community with shared concerns.

- ·*Hybrid Cloud*

This is a cloud infrastructure that is a composition of two or more clouds i.e. private, community or public.

II. DATA SECURITY ISSUE IN THE CLOUD

Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:

 Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a particular resource that has a threat or has been compromised.

According to service delivery models of Cloud computing, resources and cloud services may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.

Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

The clouds are used to share a information and resource by multiple user over the network so its very important , user must ensure the safe network and also utilize the resource allocation and scheduling provide the clouds. The security and the privacy is very important when designing and using the cloud service. So the cloud computing is enlarged way to cover the security issue, concern and challenges for Data security in cloud.

- **Data Issue**: From cloud service anyone from anywhere can access the data so protection of data is very important Issue. The following data issue are:

1. **Data privacy and confidentiality**: Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety.The cloud seeker should be assured that data hosted on the cloud will be confidential.

2. **Data Intergrity**: With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

3. **Data location and relocation**: Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information. Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others' resources.

1. **Data Availability :** Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

2. **Data storage, Backup and Recovery** : When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience gstorage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

- **Privacy Issue**: The cloud computing service provider must sure that user personal information must secure. So Authentication is one of the solution for the privacy issue.

III. EXISTING SYSTEM

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

Disadvantages of Existing Systtem:

1. Cloud providers should address privacy and security issues as a matter of high and urgent priority.
2. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

IV.PROPOSED WORK

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an un-trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

Advantages:

1. Data Integrity
2. Service Availability.
3.The user runs custom applications using the service provider's resources
4.Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.

ALGORITHM USED:

Secret Sharing Algorithms:

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. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the 2012 45th Hawaii International Conference on System Sciences file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

The goal is to divide data D (e.g., a safe combination) into n pieces $D_1, \ldots, D_n$ in such a way that:

Knowledge of any k or more D_i pieces makes D easily computable.

Knowledge of any $k-1$ or fewer D_i 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 to reconstruct the secret.

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define aparabola, 4 points to define a cubic curve and so forth. That is, it takes k points to define a polynomial of degree $k-1$.

Suppose we want to use a (k, n) threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size P where $0 < k \leq n < P$ and P is a prime number.

Choose at random $k-1$ coefficients $a_1, \cdots, a_{k-1}$ in F, and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$. Let us construct any n points out of it, for instance set $i = 1, \cdots, n$ to retrieve $(i, f(i))$. Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

Preparation

Suppose that our secret is 1234 $(S = 1234)$.

We wish to divide the secret into 6 parts $(n = 6)$, where any subset of 3 parts $(k = 3)$ is sufficient to reconstruct the secret. At random we obtain two $(k-1)$ numbers: 166 and 94.

$(a_1 = 166; a_2 = 94)$

Our polynomial to produce secret shares (points) is therefore:

$f(x) = 1234 + 166x + 94x^2$

We construct 6 points from the polynomial:

(1,1494) (2,1942) (3,2578) (4,3402) (5,4414) (6,5614)

We give each participant a different single point (both x and $f(x)$).

$$\ell_0 = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

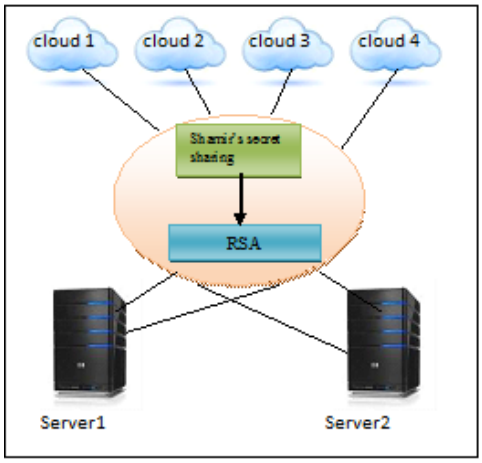
$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$=1234+166x+94x^2$

Recall that the secret is the free coefficient, which means that S=1234, and we are done.

RSSA(Ron Rivest Adi Shamir's Secret Sharing Algo)

RSSA algo will select the safe prime numbers by using Shamir Secret Algo and those prime will be used in RSA algo for encryption and decryption where K = n



1.Find safe prime no by using the Shamir's secret sharing algo
2. Shamir's secret sharing will calculate 2 safe prime no as p and q.
3. $n_{rsa} = k_{sss}$
4.Now p=p' and q= q' for security purpose ,the integers p' and q' chosen by Shamir's secret sharing algo.
5. compute n_{rsa} = p'q' n_{rsa} is used as the modulus for both public and private keys.
6.Φn_{rsa} = $\Phi(p')\Phi(q')$ =(p'-1)(q'-1) where Φ is Euler's totient function
7.Choose an integer e such that $1<e<\Phi(n_{rsa})$ and GCD(e, $\Phi(n_{rsa})$) = 1; i.e. and $\Phi(n_{rsa})$ are coprime.
8. Determine *d* as $d \equiv e^{-1} \pmod{\varphi(n_{rsa})}$; i.e., *d* is the multiplicative inverse of *e* (modulo $\varphi(n_{rsa})$).*d* is kept as the private key exponent.

Encryption:
Encryption is the process of converting original plain text (data) into cipher text (data).
Steps:
1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who want to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text(data) C is $C = m^e \pmod{n}$.
4. This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:
Decryption is the process of converting the ciphertext(data) to the original plain text(data).
Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, $m = C^d \pmod{n}$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

V. CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.
Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm. The purpose of this work is to survey the recent research on single clouds and multi-clouds using secret sharing algorithm and to address the security risks and solutions using Shamir‟ s Secret Sharing algorithm. These algorithms generate their own secret sharing schemes and use secure channels to distribute shares among themselves. The Shamir's secret sharing scheme has a good abstract foundation which provides an excellent framework for proofs and applications .

REFERENCES

1. "CLOUD COMPUTING'S EFFECT ON ENTERPRISES" Masters_Thesis_-_Cloud_Computing_-_Rehan_Saleem.pdf
2. "An Efficient data storage security algorithmusing RSA Algorithm" Amandeep Kaur1, Sarpreet Singh2.
3. "Data Security in Cloud Computing using RSA Algorithm" Parsi Kalpana, Sudha Singaraju
4. "Enhanced Security for Cloud Storage using Hybrid Encryption" Reema Gupta1, Tanisha2, Priyanka3
5. "Providing Data Security in Cloud Computing using public key cryptography" N.PADMAJA1 , PRIYANKA KODURU
6. "Using encryption Algorithms to enhance the Data Security in Cloud Computing" MANDEEP KAUR, MANISH MAHAJAN
7. "What Cloud Computing Really Means"- infoWorld.com.
8. Draft NIST Working Definition of Cloud Computing v15, http://csrc.nist.gov/groups/SNS/cloudcomputing/clouddef-v15.doc.
9. "Google App Engine "http://code.google.com/appengine/.
10. http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing
11. http://en.wikipedia.org/wiki/RSA_(cryptosystem)
12. Axel Buecker, Koos Lodewijkx, Harold Moss, Kevin Skapinetz, Michael Waidner, " Cloud Security Guidance", a red paper, January 2011.
13. Hassan Takabi, James B.D., Joshi, Gail-Joon, Ahn, "Security and Privacy Challenges in Cloud Computing Environments", University of Pittsberg, October 2010.
14. Neil Robinson, Lorenzo Valeri, Jonathan Cave and Tony Starkey (RAND Europe), Hans Graux (time.lex), Sadie Creese and Paul Hopkins (University of Warwick), "The Cloud: Understanding the Security, Privacy and Trust