IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Assured Data Storage: A Divide and Secure Multipart Algorithm for Cloud Storage

Vaikar Ameya[1*], Pawar Deepak[2] and Laddha Yogesh[3]

[1*,2,3]*Department of Computer Engineering, Late G.N.Sapkal College of Engineering, India*
ameyavaikar@gmail.com; er.deepakpawar@gmail.com; er.yogeshladdha@gmail.com

www.ijcseonline.org

Received: 11 Feb 2014 Revised: 18 March 2014 Accepted: 26 March 2014 Published: 31 March 2014

Abstract— This paper details about the single cloud and multi clouds security systems using MultiPart Secret Sharing Algorithm using Shamir's Secret and RSA algorithm and addresses possible solutions and methodology. Main focus of in this paper is on use of multi clouds and data security and reduces security risks and affects the cloud computing users using Multipart Secret sharing algorithm. It is a form of secret sharing, where a secret is divided into parts, which is giving each participant its own unique part, where some of the parts are required in order to reconstruct the secret. This algorithm is used where any "k" the parts are sufficient to reconstruct the original secret message, helping in Enhanced Security measures.

Index Terms- Cloud Computing, Multi Clouds,Multipart Secret Sharing Algorithm, Threshold, Reconstruct

I. INTRODUCTION

Cloud computing is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing is "A way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software[2]. We can classify cloud as:-

1. Public
2. Private
3. Community
4. Hybrid

II. NEED FOR THE SYSTEM

The need for the new system contains an encryption algorithm called Multi-Part Encryption Algorithm. This algorithm divides the individual's data into "k" distinct parts and encrypts it into a Quadratic equation[3]. Quadratic equations are then stored on several connected clouds for the security of the data. While decoding, the quadratic equations are again called from the connected clouds and decoded back in the original form[3]. This helps in maintaining the security of the data. The proposed system uses the MultiPart algorithm with RSA for Cryptography and provide a secure means for data storage and communication[4].

III. FEASIBILITY OF THE SYSTEM

1. *Functional:-*Easy for the user to Upload and Download Data. It provides High Level Security for confidential Data with less time.

Corresponding Author: Vaikar Ameya

2. *Technical:-*Provides an interface for the cloud user to store and retrieve the confidential data in an easy manner with highest level of security.

3. *Economical:-*It is Cost Efficient & everything comes under one package.

This project is designed developed for the user to optimally secure his/her data on the Internet. This project will provide the users with a secure and safe data storage capability and ease of use too.

IV. LITERATURE SURVEY

Recently, Cloud Computing has gained a lot of popularity in the Computer Industry[1]. Many innovative ideas have been placed like Cloud based Security, Application extensibility, etc.

1. Encryption Systems.
2. Decryption Systems.
3. Data Security measures.

Now a days rapidly increased use of cloud computing in the many organization and IT industries and provides new software with low cost. So Cloud Computing gives us lot of benefits with low cost and of data accessibility through Internet[6]. Ensuring the security factors of cloud computing is the main aspect in the cloud computing environment. Single cloud providers are less popular with customers due to the risks in service availability failure and possibility of malicious insiders in the single cloud[1]. A movement of multi clouds or multiple clouds has emerged currently using Shamir's Secret Sharing Algorithm[1]. This topic surveys to many running research paper to single cloud and multi clouds security using Shamir's Secret Sharing algorithm and the RSA algorithm and addresses possible solutions and

methodology. Main focus is use of multi clouds and data security and reduce security risks and affect the cloud computing user. It is a form of secret sharing, where a secret is divided into parts, which is giving each participant its own unique part, where some of the parts or all of them are required in order to reconstruct the secret.

V. SYSTEM ANALYSIS

Security continues to be a major challenge for cloud computing, and it is one that must be addressed if cloud computing is to be fully accepted.-[1] Most technological means of securing non-cloud computing systems can be either applied directly or modified to secure a cloud. The purpose of the system is:

1. To provide high level of security for a data which user wants to store on cloud.
2. To provide assured security to user's data with ease of use to download and upload it on the cloud without any extra efforts.
3. To provide high security to Government sites, Military data and other confidential information and protect this data from Hackers. Cloud computing concept is relatively new concept but it is based on not so many new technologies. Many of the features that makes cloud computing attractive, however has to meet certain basic security criteria. In our paper, we have briefed on various measure on cloud computing security challenges from single to multi clouds.

While making a cloud secure, the following objectives are to be met:

1. Understanding the cloud computing environment provided by the cloud service provider[4].
2. The cloud computing solution should meet the basic security and privacy requirements of any firm deploying it[6].
3. Maintain an account of the privacy of the cloud and data security and applications that are deployed in cloud computing environment[4].
4. Data Integrity.[2]
5. Service Availability.[5]

Assumptions and Dependencies

1. User must have account on following clouds:
2. Google Drive
3. Sky Drive
4. Drop Box
5. User must have his own email account.
6. User must have knowledge about internet and drive SDK's.
7. At the time of storing a data on cloud user must use our application.
8. User must have Internet connection.

This system is real time and hence should be performed in minimum time requirement. The Accountability is a vital feature and this could only be assured if the system is working in full capability. So uninterrupted power supply and uninterrupted internet connection is needed. The data stored on cloud is very vital. The server should always be confirmed to run properly and data saved to the database at consecutive interval. Power is a significant feature and the power supply should be always taken care off. A uninterrupted power supply is always recommended. The security system features from having a login for users to access the software .the login details will be used in the system also, so the changes of the software getting intruded are very less. The source code of our system is an open source software.

VI. SYSTEM IMPLEMENTATION

Data stored in the cloud can be compromised or lost[2]. 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[1]. 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[2]. 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[2].

Mathematical Definition given below:

Our goal is to divide some data D (e.g., the safe combination) into η pieces D1, D2…,Dn in such a way that:

1. The Knowledge of any k or more Di pieces makes D easily computable.
2. The Knowledge of any k-1 or fewer Di 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 original data. 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 a parabola, 4 points to define a cubic curve and so forth. That is, it takes κ points to define a polynomial of degree κ*[1]*

1. Suppose we want to use a (κ, η) threshold scheme to share our secret *S,* without loss of generality assumed to be an element in a finite field *F.*

Choose at random (κ -1) coefficients a_1, $a_{\kappa-1}$ in *F,* and let $a_0 = S$. Build the polynomial

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{k-1}x^{k-1} \quad .$$

Let us construct any η points out of it, for instance set i=1,…,$\eta$to retrieve (i, $f(i)$). Every participant is given a point (a pair of input to the polynomial and output). Given any

subset of κ of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term a_0.

Shamir Approach:
We divide our secret into pieces by picking a random degree.
The following example illustrates the basic idea. Note, however, that calculations in the example are done using integer arithmetic rather than using finite field arithmetic. Therefore the example below does not provide perfect secrecy, and is not a true example of Shamir's scheme.
Suppose that our secret is 1234(S =1234)[1] .

We wish to divide the secret into 6 parts(n=6), where any subset of 3 parts(κ =3) is sufficient to reconstruct the secret.
At random we obtain 2 numbers: 166, 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 $f(x)$).

VII. SOLUTION METHODOLOGY

Cloud customers may form their expectations based on their past experiences and organizations" needs. They are likely to conduct some sort of survey before choosing a cloud service provider[1]. Customers are expected also to do security checks that are centered on three security concepts: confidentiality, integrity and availability. On the other hand, cloud service providers may promise a lot to entice a customer to sign a deal, but some gaps may manifest later as overwhelming barriers to keep their promises. Many potential cloud customers are well aware of this, and certainly, still sitting on the sidelines[5]. They will not undertake cloud computing unless they get a clear indication that all gaps are within acceptable limits[1]. We organized cloud computing security into three sections: security categories, security in service delivery models and security dimensions[1].

Security in cloud services is based on the following:

- Strong network security is possible around the service delivery platform[2].
- Data encryption: for data in transit (particularly over wide area networks), and sometimes stored data, but it cannot be applied to data in use.
- Access controls to ensure that only authorized users gain access to applications, data and the processing environment and is the primary means of securing cloud-based services[3].
- Service providers are able to inspect activity in their environment and provide reports to clients[1].

VIII. RESULT ANALYSIS

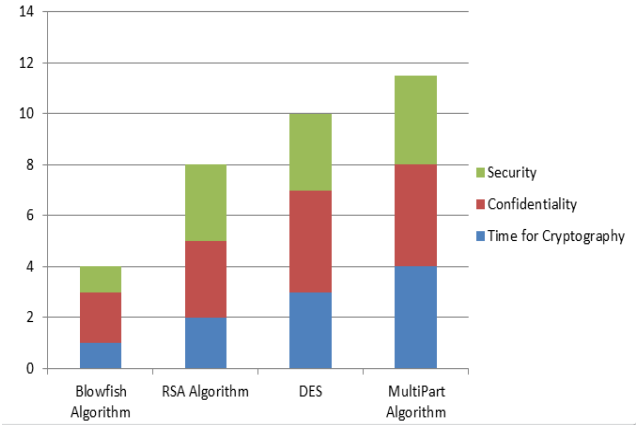

Fig.1 Comparative study between various Cryptographic Algorithms

The Blowfish, RSA, DES and MultiPart algorithms are all used for the Cryptographic analysis of the data. The blowfish algorithm has quite lower efficiency than compared to the other Algorithms. The RSA algorithm and the DES algorithm go hand in hand but the main difference between them is Keys used that result in the Confidentiality measures. The RSA algorithm provides less Confidentiality as Different keys are used for Encryption and Decryption. The MultiPart algorithm, on the other hand, is the most secure of all as it overcomes all the drawbacks of the previous algorithms. This algorithm provides same key for Cryptography, it provides more usability and avails a new concept of dividing the key in numerous parts leading to better security. Thus, rendering this algorithm to be more "Useful".

Parameters	Blowfish	RSA	DES	MultiPart
Key Used	Different key	Different key	Same key	Same key
Scalability	Keysize varies	Key size is the same	Key Size varies	Key size is the same
Throughput	Low	Moderate	High	Very high
Confidentiality	Low	Moderate	High	High

Table 1 Difference between the Cryptographic Algorithms

REFERENCES

[1] Md Kausar Alam, Sharmila Banu K, "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds.", International Journal of Scientific and Research Publications, Volume **3**, Issue **4**, April **2013** 1 ISSN 2250-3153.School of Computing Science and Engineering, VIT

University, Vellore, Tamil Nadu, India.
[2] Carlos Goncalves, Luis Assuncao, Jose C,"Data Analytics in the Cloud with Flexible MapReduce Workflows", IEEE 4th International Conference on Cloud Computing Technology and Science.
[3] Mandeep Kaur and Manish Mahajan,"Implementing various encryption algorithms to enhance the data security of cloud in cloud computing", VSRD International Journal of Computer Science &Information Technology, Chandigarh Engineering College, Mohali, Punjab, INDIA, Vol**. 2** No. **10** October **2012 /** 831ISSN No. 2231-2471 (Online), 2319-2224 (Print)
[4] SafeGuard Encryption for Cloud Storage.
[5] Available at http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing.