Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

Enhanced cloud Data recovery technique using Seed Block Algorithm (SBA) and RSA Encryption

D.A Phalke, Onkar Kulkarni, Abhijit Fulsagar,Harish Rane, Ajinkya Chothave
D.Y.Patil College of Engineering, Akurdi, Pune-411044, Maharashtra, India.

REVIEW ARTICLE

Received on: 18-03-2014
Accepted on: 01-04-2015
Published on: 08-04-2015

D.A Phalke, Onkar Kulkarni, Abhijit Fulsagar,Harish Rane, Ajinkya Chothave
D.Y.Patil College of Engineering, Akurdi, Pune-411044,
Maharashtra, India
a_dhanashree@rediffmail.com,kulkarniosk@gmail.com,abhijitfulsagar@gmail.com,hrane1994@gmail.com, ajinkya.ac@gmail.com

QR Code for Mobile users

Conflict of Interest: None Declared

ABSTRACT

Cloud computing is increasing day by day as its advantages overcome the disadvantage of various early computing techniques. Cloud provides huge amount of online data storage where data is stored. Clients store their valuable private data in the cloud for future use. If in case, file deletion or if the cloud gets destroyed due to any reason the data stored at cloud gets lost. Hence to overcome this problem data recovery technique have been developed in cloud computing. Various recovery techniques are developed to tackle this problem in the previous years. Our system is also based on data recovery technique which can be used to backup cloud data and recover that data. The proposed system is based on the Seed Block Algorithm (SBA) and RSA encryption

Keywords: Cloud Computing, Seed Block Algorithm (SBA), RSA, Backup, Recovery

Cite this article as:
D.A Phalke, Onkar Kulkarni, Abhijit Fulsagar,Harish Rane, Ajinkya Chothave. Enhanced cloud Data recovery technique using Seed Block Algorithm (SBA) and RSA Encryption. Asian Journal of Engineering and Technology Innovation 03 (06); 2015; 39-43.

INTRODUCTION

Today, Cloud Computing is itself a gigantic technology which is surpassing all the previous technology of computing. Cloud computing is increasing day by day because of its advantages. It is evolved much, because it is able to store huge amount of data. This data which is uploaded by various users/clients is valuable information. Another important advantage is its flexibility to store data on cloud and its easiness to access the data. Since today users seek for comfort level. Thus cloud computing must be able to provide reliability, so that users can upload their sensitive and important data. As cloud is very flexible and easy to use, thus it becomes very important to provide security to the valuable data which client uploads.

There are few challenges like Security and Privacy, associated with this computing model which may cause a slow-down while delivering the services effectively in the cloud computing. Cloud Disaster is one of the most important factors in Cloud Computing. As number of user shares the storage and Other resources, it is possible that other customers can access your data. Either the human error, cloud damage faulty equipment's, network connectivity, a bug or any criminal intent may put our cloud storage on the risk and danger. Thus, recovery technique must be there so that client can get back its own data safely. The recovered data must be complete and fair data. And it must not take time. Thus data security and recovery becomes very important part when it comes to cloud computing.

In literature many existing techniques have been explained like HSDRT, PCS[5], ERGOT[6], Rent out Of Service[7] etc. However, still various successful techniques are lagging behind some critical issues like low cost,implementation complexity, security and time related issues. To tackle this issues, in this paper we have used a smart remote data backup algorithm, Seed Block Algorithm (SBA). And to provide security additionally and encryption technique is used.

LITERATURE REVIEW

In literature, we study most of the recent back-up and recovery techniques that have been developed in cloud computing domain such as HSDRT, PCS[5], ERGOT[6], and Rentout Of Service[7].

Parity Cloud Service (PCS)[5] is a very simple, easy to use and more convenient for data recovery which is based on parity recovery service. A PCS has low cost for recovery and can recover data with very high probability. For data recovery, PCS uses a new technique of generates a virtual disk in user system for data backup, parity groups are created across virtual disk, and store parity data of parity group in cloud. It uses the Exclusive–OR ( ) for creating Parity information. It is comparatively Simple, reliable, easy to use and more convenient for data recovery. But the limitation is, it is complex to implement.

ER-GOT[6] is based on the Semantic Overlay Network (SON) and Distributed Hash Tables (DHT). It provides an efficient retrieval of data that is completely based on the semantic similarity between service descriptions and service requests. It promotes scalability as well as semantics to enable their precise and efficient data retrieval. Advantage of ER-GOT is fast and exact match data retrieval and Privacy to data, and disadvantage is High time and implementation complexity

Rent out the Rented Resources [7] is based on renting the resources to clients in form of cloud service. It aims to reduce the monetary cost of cloud services. Here a third party is involved, which rents the resources to the clients. This third party is in contact with the client as well as the actual owner of the resource. It is based on three core objectives, firstit minimizes the cloud infrastructure cost, and secondit provides low cost cloud services by reducing infrastructure cost for the cloud vendors to the clients, third it gives the monetary benefit with the large under-utilized technology infrastructure to the established enterprises. Its limitation is Resources must be kept under special attention due to rented concept.

HS-DRT[2] makes use of an effective ultra-widely distributed data transfer mechanism and a high-speed encryption technology, based on the assumption that we can use a small portion of the storage capacity of a large number of PCs and cellular phones that are in use in daily life, to efficiently realize safe data backup at an affordable maintenance and operation cost. This technique can be used by movable clients like smartphones, laptop etc. Since data is distributed widely, it cost high implementation.

Ulteo Open Virtual Desktop[9]it is an open source application delivery.it can deliver application or desktop hosted on Linux or windows server to end user. It is like virtual cloud. Number of clients can access specific application or entire Desktop through OVD[9].

Remote data backupServer [1] is mostly used for storing back up replica of file which is going to be deleted. So in future if client require this file he can easily restore from backup server. Client store the file on cloud but by mistake file is deleted from cloud then it gets impossible to restore file again if backup server not there. For purpose of user comfort we have to implement Remote backup server for the cloud. It is going to work in two way,

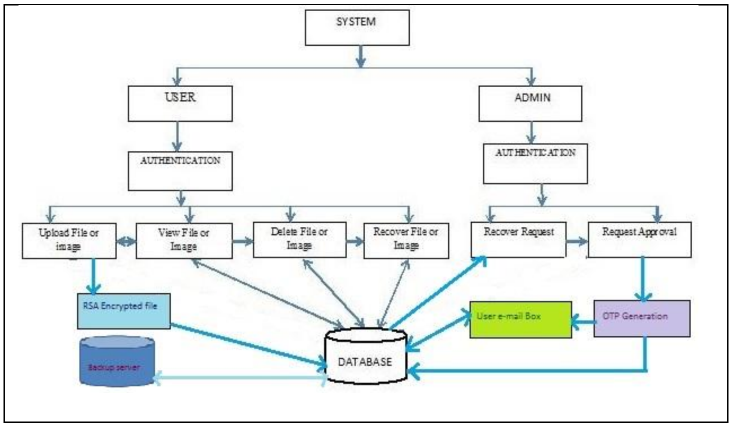
1. If file deleted from cloud
2. If cloud get crash due to any reason

If file is deleted from the cloud then this file is store on backup server. When user ask specific file which is not on cloud then it used to search in backup server. It trace the file in backup server and restore file again into cloud. In other case if cloud gets crash then all the file in cloud gets store on the backup server and after installation of new cloud all the file of backup server restore to new cloud.

OTP code securitymeans One Time Password. It is most of the time used for the security purpose. In our system we used OTP for providing security. When user want to view file or recover file from backup server to cloud then system generate OTP code and send to the registered email id. Then user have to access email account for getting OTP. After providing OTP, User can view file or file get restored to cloud. OTP is generated from the random number.

OTP recover from registered email account so alternatively we provide two steps verification in our security constraint. This is main advantage of using OTP code generation in system.

PROPOSED SYSTEM ARCHITECTURE



Working of System:

The total system works on the "Seed Block algorithm". In the System we can see there are two main modules as 1st is user and 2nd is admin. Now user and admin enters into their authorized area so both of them goes through authentication process. After getting into "seed block" user can do his/her desired utilization as user can upload, view, Delete and Recover. The deleted file gets store on the backup server.

When user uploads the file, the file goes through RSA encryption and file gets store into the database where user can view, delete that file.

When user wants to recover file, he requests system to recover where admin alias the system accepts request generates OTP i.e. Dynamic password and sends it to user's e-mail box and database. So when user enters that OTP into system then only we can get our file back.

MATHEMATICAL MODEL

- C: Cloud {Ad,Us}
  - Us: User {Fv, Fu, Fd, Fr}
  - Ad : Admin {Frr, Fra}

Where Fv: File view, Fu: File upload, Fd: File delete, Fr: File recovery,Ftxt : File in txt format,Frr : File recovery request ,Fra : File recovery approval

Initialization: Main Cloud: Mc, Remote Server: Rs, Clients of main cloud: Ci, Files: a1 and a1', Seed Block: Si, Random number: r, Client's Id: Client_Idi

Input: a1 is created by Ci; r is generated at Mc;

Output: Recovered file a1 after deletion at Mc or on user's request

Given: Authenticated clients are allowed to upload, download and do modification on its own files only.

```
1. Generate random number.
        int r =rand();
2. Create a Seed Block Si for each Ci and store Si at Rs
        Si= r XOredClient_Idi
3. If Ci creates/modifies a1 then store at Mc,then a1' is created as
        a 1'= a1 XORed Si
4. Store a1 at Mc and Rs
```

5. If user request for a deleted file or server crashes a1 from Mc, then we do EXOR to retrieve the original a1 as:
    a1=a1'XORed Si
6. Return a1 to Ci
7. END

DATASET

In our System Dataset we include memory size requirement and limitation. For main cloud server we required 5GB. We can increase it as per requirement. We put 8 GB for Remote back-up server. Back-up server store more data than cloud so required more memory than cloud.

We provide limitation for uploading file size. File size up to 1MB is allowed to upload. File size greater than 1 MB,system is not accept it. For fast upload data and working of system we provide this limitation.

ALGORITHMS

RSA Encryption Algorithm

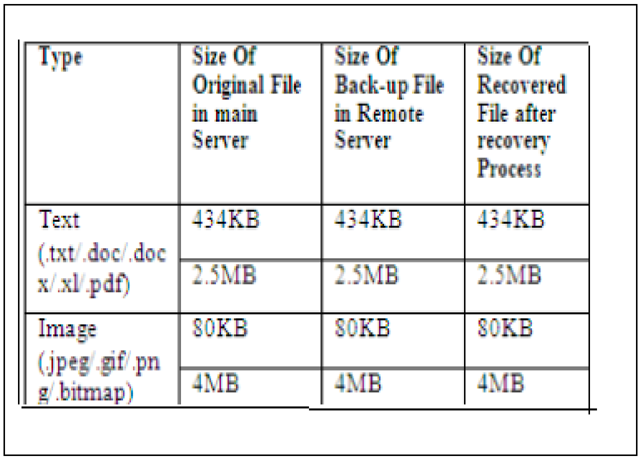
1. Given an integer key size 1<=k<=4000, generate random prime large Integers p, q with k bits; let n = pq and generate random large Integer d such that p,q < d < n and relatively prime to (p-1)(q-1). Let e = inverse of d mod (p-1)(q-1). Save p, q, d in hexadecimal format.
2. Given two prime large Integers set p, q = these (check their primality) and generate d, e as in 1. Save p, q, d in hex format.
3. Given p, q, d, check primality of p, q; check p, q < d < pq and GCD(d, (p-1) (q-1)) = 1 and if ok, generate e = inverse of d mod (p-1)(q-1). Save p, q, d.
4. Read p, q, d and compute e = inverse of d mod (p-1)(q-1).
5. Divide input data into x blocks
6. Add padding bits into x blocks
7. Convert blocks into integer and calculate exponential value e
8. Calculate modulus n of above calculated value
9. Repeat process for all blocks to generate encrypted data
10. For decryption, Divide input data into x blocks
11. Add padding bits into x blocks
12. Convert blocks into integer and calculate exponential value using key d
13. Calculate modulus n of above calculated value
14. Repeat process for all blocks to generate decrypted data

EXPECTED RESULT:

Memory requirement is kept 5GB and 8GB for the main cloud's server and remote server respectively, which can be extended as per the necessity, it is observed that memory requirement is more in remote server as compare to the main cloud's server because additional information is placed onto remote server.

Parameter	Cloud Server	Remote Server
CPU	I3 Processor	I3 Processor
Memory	5GB	8GB
OS	Windows, Linux	Windows, Linux
HDD	500 GB	500GB

Our expectation that size of original data file stored at main cloud is exactly similar to the size of Back-up file stored at Remote Server. For this purpose we perform this experiment for different types of files. Proposed SBA with RSA encryption is very much robust in maintaining the size of recovery file same as that the original data file. RSA encryption technique gives data security form encrypted file. From this we expected that proposed SBA recover the data file without any data loss as well as provide encryption to file after uploading.



Type	Size Of Original File in main Server	Size Of Back-up File in Remote Server	Size Of Recovered File after recovery Process
Text (.txt/.doc/.docx/.xl/.pdf)	434KB	434KB	434KB
	2.5MB	2.5MB	2.5MB
Image (.jpeg/.gif/.png/.bitmap)	80KB	80KB	80KB
	4MB	4MB	4MB

CONCLUSION

In this Paper, We presented detail design of SBA and RSA algorithm. Proposed SBA helping users to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. RSA Encryption focuses more on security concepts. Proposed recovery system overcome the time related issues such that it will take minimum time for recovery process.

REFERENCES

1. Ms. Kruti Sharma, Prof. Kavita R Singh,"Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies.
2. Ms..Kruti Sharma,Prof K.R.Singh, 2012, "Online data Backup And Disaster Recovery techniques in cloud computing:A review", IJEIT, Vol.2, Issue 5.
3. Chintureena Thingom, "Cloud Disaster Management With Scheduling Strategy", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 3, Issue 5, May 2014, ISSN: 2277 – 9043
4. Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications", Fifth International Conference on Systems and Networks Communications, 2010, pp 256-259.
5. Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, 2011, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.