iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improved Cloud Back-Up System

Prof. V.S.More[1], Ketan Pandit[2], Shraddha Kadam[3], Prasad Shinde[4]
[1,2,3,4]*Department of Computer Engineering, RMCET, Mumbai, India*

Abstract: Nowadays cloud computing is most widely used technique in the world. In cloud computing, data is generated over the cloud is in electronic form. To maintain this large data efficiently we required data recovery services. In this paper we propose a remote data backup algorithm, Seed block algorithm (SBA), advanced encryption Standard (AES), MD5 algorithm. This Algorithm is useful for user to collect information from any remote location and if any file gets deleted or if the cloud get destroyed due to any reason then the SBA algorithm will helps to recover the file. Also it will take minimum time for data recovery process i.e. it solves the time related issue. Proposed SBA also focuses on security concept for the backup the files stored at remote server.

Keywords : Seed Block Algorithm (SBA), Advanced Encryption Standard (AES),Cloud Back-up. Remote Cloud, Main Cloud, MD5.

I. INTRODUCTION

When we heard the word cloud computing then one question is arises that is What is the cloud? Where is the cloud? Are we in the cloud now? These are all questions you've probably heard or even asked yourself. The term "cloud computing" is everywhere. In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. In today's world the need of cloud computing increases day by day because its advantages overcome the disadvantage of various previously developed computing technique, like grid or cluster computing. Cloud storage provides online storage where data is shared in form of virtualized pool that is usually hosted by third parties. The hosting company operates large data on large data center and according to them as the storage pools that help use to share file or data objects. In this situation number of users shows the same cloud storage provided by a certain service provider. Then it is possible that other customer can access your data. To solve the problem of data loss we need to provide data integrity for our cloud .There are many techniques previously implemented like PCS[1], HSRDT[2], Linux Box[3], ERGOT[4] etc. Which are used for data recovery process? There are some critical issues of these techniques like implementation complexity, low cost, security and time related issue.

To overcome these issues we have proposed a new method using Seed Block Algorithm, Advanced Encryption Standard Algorithm, and MD5. The procedure of this technique works as follows: In first step it allows user to collect and store their files onto the main cloud. As soon as the files get stored onto the main cloud, these file get encrypted using AES Algorithm. In step two, if file gets deleted due to any reason it helps server to recover the files.

II. LITERATURE SURVEY

In literature Survey we studied the existing method in detail. On the basis of that survey we found that, the actual working of that system is not satisfied as compared to cost. This system has low security complexity and takes lot of time to produce output on given input.

A. Parity Cloud Service

PCS is more reliable, easy to use and more useful for data recovery based on parity recovery service. PCS generates virtual disk in a user system for data backup. It makes parity group across the virtual disk and store parity data in it parity group in cloud to recover it. For all of this operation it use Ex-Or operation to store data for backup. There are some problems related to this system are unable to control implementation complexity.

B. HSRDT(High Security Distribution & Rate Technology)

HSRDT is more powerful technique for movable clients such as laptop, smart devices etc. Drawbacks of this system are it take more cost for implementation and also generate the repeated backup file in remote backup server (i.e. replication of data).

C. Linux Box

We observed that this technique is having simple data backup and recovery with very low cost. Drawback of this system is

security is very low and transformation of information from one cloud services to another to be very easy. Also the limitation we found that it take backup of not only the data but also take backup of entire virtual machine causes the wastage of bandwidth.

D. ERGOT(Efficient Routing Grounded on Taxonomy)

The system is semantic based system which helps for service discovery in cloud computing. Basically ERGOT works on semantic analysis. But it fails to focus on time constraints & complexity related to implementation

ERGOT is built using three components,

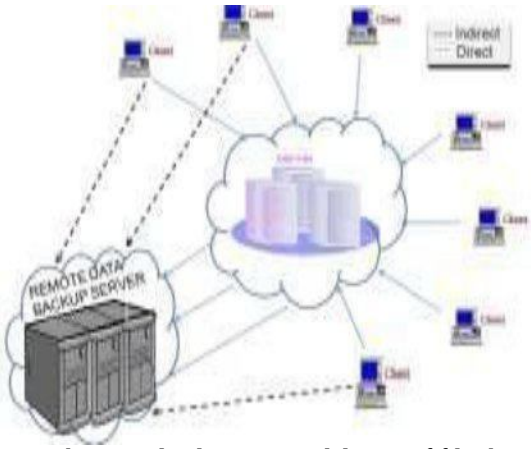
A DTH (Distributed Hash Table) protocol.

A SON (Semantic Overlay Network)

A measure of semantic similarity among service description.

III. REMOTE DATA BACKUP SERVER AND ITS ARCHITECTURE

When we study on Backup Server of main cloud, we only focus on the replica of main cloud server. At certain state backup server is at remote location and main cloud, and then this severs is known as remote Data Backup Server.



If user losses its data because of human attack, natural calamities or deletion of file then it gets its file from remote server. The main purpose of the remote backup server is to help user to collect information from any remote location even if data is not available on main cloud.

The Remote Backup Services should fulfill the following aspects:

A. Data Confidentiality

User's data should be kept confidential when no. of clients simultaneously operates the same server. Data which is personal to only specific users must be kept secure from other users on the cloud during the transmission of data or accessing the data.

B. Data Integrity

Data integrity says that during the transmission or reception of file, data should remain unaltered. It mainly focuses on validity and fidelity of the data.

C. Data Security

Data security gives first priority for the remote server is protection of client's data. In data security user's data should be not able to access by third party.

D. Trustworthiness

Clients store their personal data on main cloud, so the main cloud and the remote back-up cloud should be trustworthy.

E. Cost Efficiency

The cost of recovery should be minimum. As the cost of recovery is less, then the system's rating will be better.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. DESIGN OF THE IMPLEMENTED SYSTEM

To overcome the disadvantage of previously implemented techniques we have proposed a new system which makes use of Seed Block Algorithm, Advanced Encryption Standard and MD5 Hash Algorithm.

A. Advanced Encryption Standard

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in block of 128 bits using cryptographic keys of 128, 192, 256 bits respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and receiver must know and use of same secret key. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that includes substitution, exchange and mixing of the input plaintext and transform it into the final output of cipher text.

B. Seed Block Algorithm

This algorithm focuses on the back-up and recovery process. It basically uses the concept of Exclusive–OR (XOR) operation. For ex: - Suppose there are two data files: A and B. When we XOR A with B, it produced X i.e. X =AB. If suppose A data file get destroyed and we want our A data file back then we are able to get A data file back, then it is very easy to get back it with the help of B and X data file .i.e. A = XB.

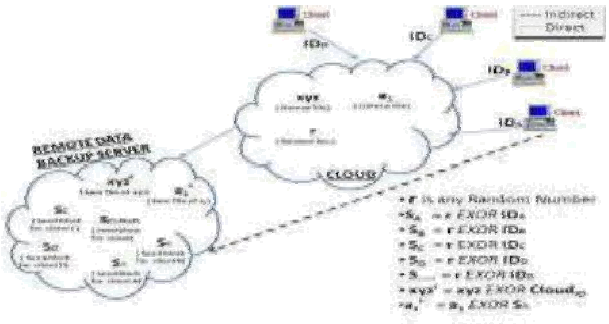


Fig.1: Seed Block Algorithm Architecture

Similarly, the Seed Block Algorithm works to provide the Back-up and recovery process. Its architecture is shown in Fig-1 consists of the Main Cloud and its clients and the Remote Server. first we set a random number in the cloud and unique client id for every client. Second, whenever the client id is being register in the main cloud; then client id and random number is getting EXO-Red () with each other to generate seed block for the particular client. The generated seed block corresponds to each client is stored at remote server.

Whenever client creates the file in cloud first time, it is stored at the main cloud. When it is stored in main server, the main file of client is being EXOR-Ed with the Seed Block of the particular client. And that EXOR-Ed file is stored at the remote server in the form of file' (pronounced as File dash). If either unfortunately file in main cloud crashed/damaged or file is been deleted mistakenly, then the user will get the original file by EXOR-ing file' with the seed block of the corresponding client to produce the original file and returns the resulted file i.e. original file back to the requested client. The architecture representation of the Seed Block Algorithm is shown in the Fig.1.

<u>The proposed SBA algorithm is as follows:</u>

Initialization: Main Cloud: Mc;
Remote Server: Rs;
Clients of Main Cloud: Ci;
Files: a1and a1'
Seed block: Si;
Random Number: r;
Client's ID: Client_idi

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

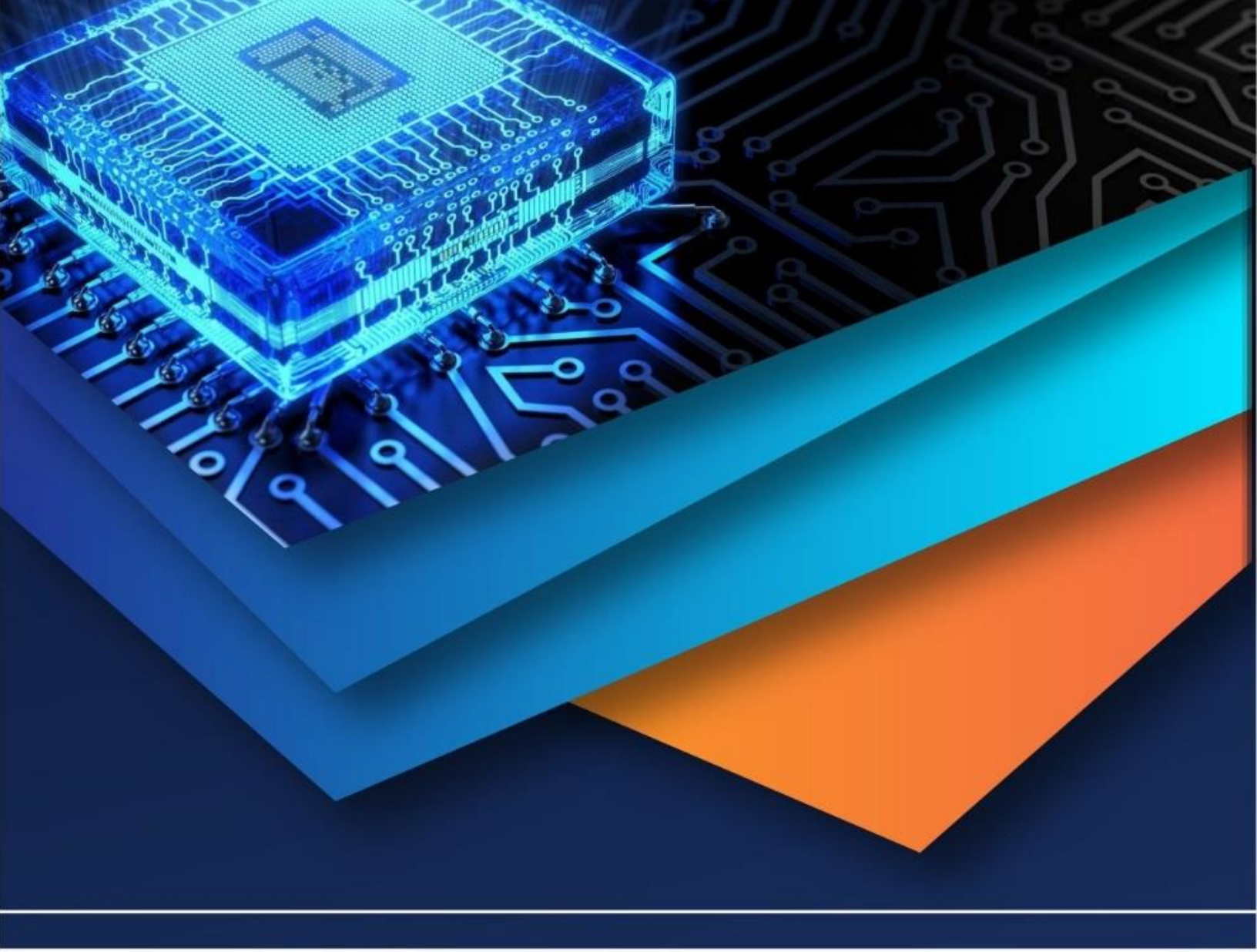
Output:
Recovered filea1after deletion at Mc
Given:
Authenticated clients could allow uploading, downloading and do modification on its own the files only. Step 1:
Generate a random number.
int r = rand( )
Step 2: Create a seed Block: Si for each Ci and Store Si at Rs -
(Repeat step 2 for all clients)
Step 3: If Ci/ Admin creates/modifies aa1and stores at Mc, Then
a1'create as
a1'= a1 Si
Step 4: Store a1'at Rs.
Step 5: If server crashes a1deleted from Mc Then, we do EXOR to retrieve the original a1 as:
a1= a1'Si
Step 6: Returna1toCi
Step 7: END.

V. CONCLUSION

In this Paper, we presented detail design of proposed SBA algorithm. Proposed SBA is robust in helping the users to collect information from any remote location in the absence of network connectivity and also to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. The time related issues are also being solved by proposed system by using SBA algorithm such that it will take minimum time for the recovery process.

REFERENCES

[1] http://www.ijtra.com/view/intelligent-cloud-security-back-up-system.pdf
[2] www.ijeert.org/pdf/v2-i7/11.pdf
[3] http://www.ijarcce.com/upload/2015/march-15/IJARCCE%2025.pdf
[4] http://www.academia.edu/8263647/Seed_Block_Algorithm_A_Remote_Smart_Data_Back-up_Technique_for_Cloud_Computing
[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.
[6] Yoichiro Ueno, Noriharu Miyaho,Shuichi Suzuki,Muzai Gakuendai, Inzai-shi,Chiba,KazuoIchihara,2010, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications,pp 256-259.
[7] Vijaykumar Javaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS),2011, "Backup for Cloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY