Data Security and Privacy in Cloud using RC6 Algorithm for Remote Data Back-up Server

Ruchira. H. Titare[1], **Prof. Pravin Kulurkar**[2],

[1] *2nd year Mtech CSE, Vidarbha Institute of Technology, Nagpur, India,* ***ruchira1302@gmail.com***
[2] *Assistant Professor, Vidarbha Institute of Technology, Nagpur, India,* ***pravinkulurkar@gmail.com***

Abstract

Cloud computing is said to be the succeeding vast thing in the world of computer after the internet. Cloud computing *means a type of Internet-based computing which provides the online storage. In cloud computing, data is generated in electronic form which is very large in amount. The cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. When data is distributed it is stored at more locations increasing the risk of unauthorised physical access to the data. As the data is stored online and in distributed form there is necessity of data recovery services in the cloud and to maintain the data integrity, we need to provide security. In this paper we provide a secured data back-up technique for cloud computing. The objective of proposed techniques is, first it helps the users to recover their data files if the file gets deleted from main cloud or if the cloud is destroyed due to any reason and second is to provide the security to user data during storage on main cloud by using RC6 encryption algorithm. The time and memory space related issues are also being solved by proposed techniques.*

Keywords: RC6 encryption, data integrity, data back-up, data recovery

---***---

1. INTRODUCTION

In today's world, there is a huge increase in the electronic data which requires large data storage devices to store this huge amount of data. These requirement leads to introduction of high storage HDD. Therefore, user prefers to store large amount of private data in cloud. Cloud storage provides the online storage where data stored in form of virtualized pool that is usually hosted by third parties. If cloud will be corrupted or damaged it leads to the loss of all important and private data then there should be some mechanisms to take back-up of the data, and provide the data at the time of cloud failure or loss of data. The data files regarding clients are stored in any hardware devices which can be lost due to hardware problem like if the system gets physically crashed or data gets corrupted then there is no other source to recover it. There are lots of chances that the errors can occur in maintaining the various users and also there is large data storage problem in centralized system.

Today, Cloud Computing is itself a massive technology which is surpassing all the previous technology of computing of this competitive and challenging IT world [1]. The cloud computing provides greater flexibility and availability of computing resources at lower cost. Cloud computing lets you access all your application and document from anywhere in the world. The hosting company operates large data on data centre and according to the requirements of the user these data centre virtualized the resources and expose them as the storage pools that help user to store files or data objects. Data sharing becomes a standard feature in most cloud storage offerings, including Dropbox, iCloud and Google Drive [2]. As number of user shares the storage, it is possible that other customers can access your data. Either the human error, faulty equipment's, network connectivity, a bug or any criminal intent may put our cloud storage on the risk and danger [11].

In literature many techniques have been proposed SBA[1], PCS[3], E-health care[4], ERGOT[6] etc. that, discussed the data recovery process.The data integrity in cloud storage, however, is subject to uncertainty as data stored in the cloud can easily be lost or corrupted due to the unavoidable hardware/ software failures and human errors. To make this matter even worse, hosting company needs to inform users about these data errors in order to maintain the reputation of their services and avoid losing profits. If the data is lost from main server and there is no other backup facility to restore this data. Then this application provides a feasible solution that collects data and sends it to a user.

To overcome these issues, we propose a new technique in which we create the back-up of data in the remote cloud. If the data on main cloud gets destroyed or data is lost then the remote cloud will give the back-up of that data to the client. The admin panel will provide a secure ID to each client which will preserves the privacy of the clients. Also the data is store on cloud by encrypting original data which provides security to the user's data.

2. RELATED LITERATURE

In literature, we study most of the recent back-up and recovery techniques that have been developed in cloud computing domain. The SBA technique help the users to collect information from any remote location in the absence of network connectivity and to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason [1].
Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud is a novel privacy-preserving mechanism to audit the correctness of shared data [2]. The Parity Cloud Service (PCS) technique provides a privacy-protected personal data recovery service [3].
The objective of Remote Data Collection Server: E-Health Care collects data and send to a centralized repository in a platform independent format without any network consideration [4].
Efficient Routing Grounded on Taxonomy (ERGOT) is totally based on the semantic analysis and unable to focus on time and implementation complexity [6].

All these techniques tried to cover different issues maintaining the cost of implementation but it creates the large amount of data and requires more storage as the size of data is not reduced. Also there is lack of privacy and security in these techniques.

3. PROBLEM DEFINITION

In the cloud, large amount of the user's personal data are stored but due to the failure of server or deletion of file then the private data of the user will be lost. This paper will explain the process of cloud creation and data storage on cloud. The user is allowed for data storage only when authentication is made by admin panel.

As data is shared in the cloud so to provide the privacy to the user we provide ID to user through the admin panel to authenticate the user.
We are also providing security to the user's data by using RC6 encryption algorithm.

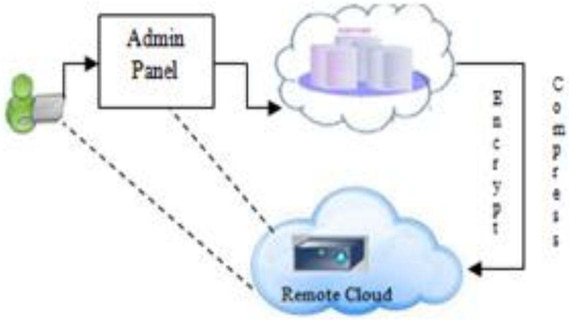


Fig.2. Architecture of Priva cy Preserving lata distribution and data back-up in remote cloud

4. PROJECT OBJECTIVES

The objective of proposed techniques is :
- To help the users to collect and recover the files in case of the file deletion
- To recover files if the cloud gets destroyed due to any reason
- To provide user friendly and secure data storage on cloud by Rc6 encryption.
- Privacy of user is maintained by providing a key to the user through admin panel.

5. INVESTIGATIONAL OUTCOME OF PROPOSED WORK

As discussed in literature, many techniques have been proposed for recovery and backup As discussed above low implementation complexity, low cost, security and time related issues are still challenging in the field of cloud computing. So in this technique we are providing the secure authentication to each user

5.1 Overview:

To achieve the objective of proposed technique, we have created a web application. In this we are providing the registration form to the user. After user is registered successfully, the data is send to the admin.

The admin then monitors the data and provide the authentication to the user. The admin send the key to the registered email ID of the user. After entering this key during login, the user's account will be activated. Then only user is allowed to upload data on the cloud.

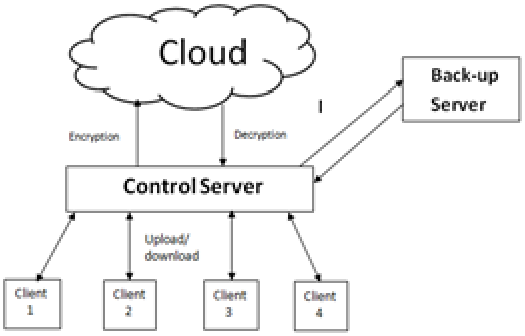


Fig 2. Secure data storage on cloud

5.2 Algorithm:

Initialization: Main cloud: M_c

Client on Main cloud: C_i
Client ID: C_id_i, Password: psw_i
Admin: A, Client's Key: K_i
File to upload: F_i
Encrypted File: E_i
Decrypted file : D_i

Step 1: Create Client Registration Form containing all the fields of client details.

Step 2: After the successful registration of Client C_i, the Admin panel A provides the key K_i for activation of Client's C_i account.

Step 3: If the client is Authenticated then only client can login by entering Client $ID\ C\_id_i$, Password psw_i and Key K_i.

Step 4: The client Ci can upload any file F_i so as to access anywhere.

Step 5: The Main Cloud M_c , stores the file F_i on the central server in the encrypted manner.

5.3 RC6 Cipher Algorithm:

For encrypting and decrypting the file we are using the RC-6 algorithm. RC6 is a symmetric key block cipher derived from RC5. RC6 has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. It is very similar to RC5 in structure, using data-dependent rotations, modular addition and XOR operations; which could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits. In this algorithm, 128 bit plaintext is divided into four 32-bit blocks and then manipulated with the keys to generated cipher text.

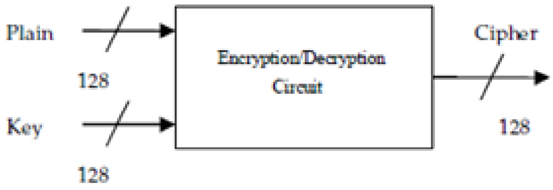


Fig 3. RC6 block cipher algorithm

The user supplies a key of 'b' bytes and the number of rounds 'r'. From this, (2r+4) words (w bits each) are derived and stored in the array S [0… 2r+3]. This array is used in both encryption and decryption.

5.3.1 Encryption

Input:

- Plain text stored in four w-bit input registers A, B, C, D
- Number of rounds 'r'
- w-bit round keys S[0, … ,2r + 3]

Output:

- Cipher text stored in A, B, C, D

Procedure:

```
B = B + S [0]
D = D + S [1]
for i = 1 to r do
{
  $t = (B * (2B + 1)) <<< \log w$
  $u = (D * (2D + 1)) <<< \log w$
  $A = ((A \oplus t) <<< u) + S[2i]$
  $C = ((C \oplus u) <<< t) + S[2i+ 1]$
  $(A, B, C, D) = (B, C, D, A)$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$
```

5.3.2 Decryption

Input:

- Cipher text stored in four w-bit input registers A, B, C, D
- Number of rounds ‘r’
- w-bit round keys S[0, … 2r + 3]

Output:

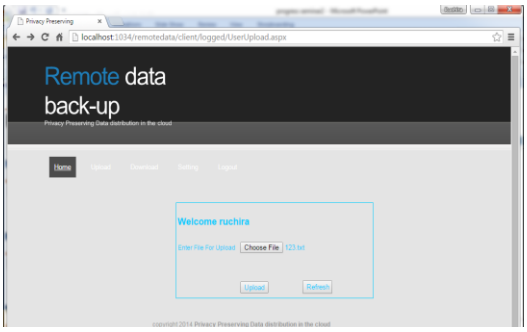
- Plaintext stored in A, B, C, D

Procedure:

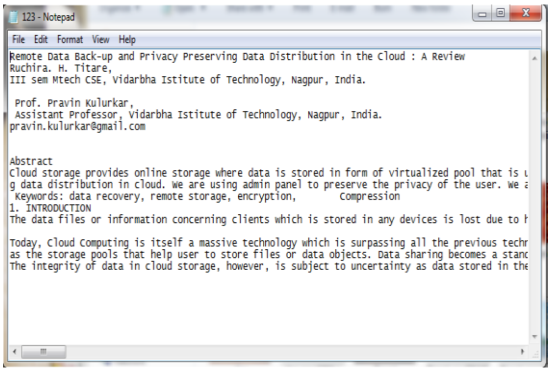
```
$C = C – S[2r + 3]$
$A = A – S[2r + 2]$
for i = r downto 1 do
{
  $(A, B, C, D) = (D, A, B, C)$
  $u = (D * (2D + 1)) <<< \log w$
  $t = (B * (2B + 1)) <<< \log w$
  $C = ((C – S[2i + 1]) >>> t) \oplus u$
  $A = ((A – S[2i]) >>> u) \oplus t$
}
$D = D – S[1]$
$B = B – S[0]$
```

5.4 Generated Outcomes:

i) File uploading:


Privacy Preserving
localhost:1034/remotedata/client/logged/UserUpload.aspx
Remote data
back-up
Privacy Preserving Data distribution in the cloud
Home
Upload
Download
Setting
Logout
Welcome ruchira
Enter File For Upload
Choose File
123.txt
Upload
Refresh
copyright 2014 Privacy Preserving Data distribution in the cloud

ii) Original file:



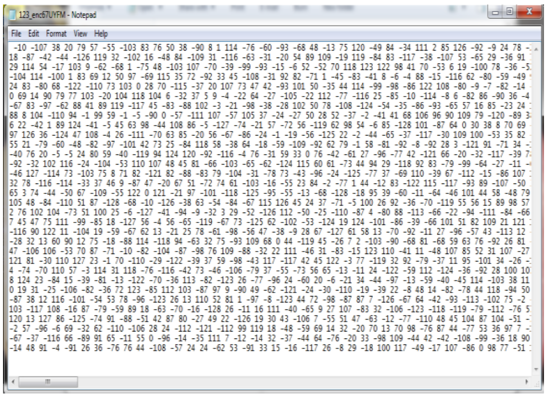
```
Remote Data Back-up and Privacy Preserving Data Distribution in the Cloud : A Review
Ruchira. H. Titare,
III sem Mtech CSE, Vidarbha Istitute of Technology, Nagpur, India.

 Prof. Pravin Kulurkar,
 Assistant Professor, Vidarbha Istitute of Technology, Nagpur, India.
pravin.kulurkar@gmail.com


Abstract
Cloud storage provides online storage where data is stored in form of virtualized pool that is u
g data distribution in cloud. We are using admin panel to preserve the privacy of the user. We a
 Keywords: data recovery, remote storage, encryption,        Compression
1. INTRODUCTION
The data files or information concerning clients which is stored in any devices is lost due to h

Today, Cloud Computing is itself a massive technology which is surpassing all the previous techn
as the storage pools that help user to store files or data objects. Data sharing becomes a stanc
The integrity of data in cloud storage, however, is subject to uncertainty as data stored in the
```

iii) Encrypted file :



```
 -10 -107 38 20 79 57 -55 -103 83 76 50 38 -90 8 1 114 -76 -60 -93 -68 48 -13 75 120 -49 84 -34 111 2 85 126 -92 -9 24 78 -
18 -87 -42 -44 -126 119 32 -102 16 -48 84 -109 31 -116 -63 -31 -20 54 89 109 -19 119 -84 83 -117 -38 -107 53 -65 29 -36 91
29 114 54 -17 103 9 -62 -68 1 -75 48 -103 107 -70 -39 -99 -93 -15 -6 52 -52 70 118 123 122 98 41 70 -53 6 19 -100 78 -36 -5
-104 114 -100 1 83 69 12 50 97 -69 115 35 72 -92 33 45 -108 -31 92 82 -71 1 -45 -83 -41 8 -6 -4 88 -15 -116 62 -80 -59 -49
24 83 -80 68 -122 -110 73 103 0 28 70 -115 -37 20 107 73 47 42 -93 101 50 -35 44 114 -99 -98 -86 122 108 -80 -9 -7 -82 -14
0 69 14 90 79 77 103 -20 104 118 104 6 -32 37 5 9 -4 -22 64 -27 -105 -22 112 -77 -116 25 -85 -10 -114 -8 6 -82 86 -90 36 -4
-67 83 -97 -62 88 41 89 119 -117 45 -83 -88 102 -3 -21 -98 -38 -28 102 50 78 -108 -124 -54 -35 -86 -93 -65 57 16 85 -23 24
88 8 104 -110 94 -1 99 59 -1 -5 -90 0 -57 -111 107 -57 105 37 -24 -27 50 28 52 -37 -2 -41 41 68 106 96 90 109 79 -120 -89 3
6 22 -42 1 89 124 -41 -5 45 63 98 -44 108 86 -5 -127 -74 -21 57 -72 56 -119 62 98 54 -6 85 -128 101 -87 64 0 30 38 8 70 69
97 126 36 -124 47 108 -4 26 -111 -70 63 85 -20 56 -67 -86 -24 -1 -19 -56 -125 22 -2 -44 -65 -37 -117 -30 109 100 -53 35 82
55 21 -79 -60 -48 -82 -97 -101 42 73 25 -84 118 58 -38 64 -18 -59 -109 -92 62 79 -1 58 -81 -92 -8 -92 28 3 -121 91 -71 34 -
-40 76 20 -5 -5 24 80 59 -40 -119 94 124 120 -92 -116 -4 76 -31 59 33 0 76 -42 -61 27 -96 -77 42 -121 66 -20 -32 -117 -39 7
-92 -32 102 116 -24 -104 -53 110 107 48 45 81 -66 -103 -65 -62 -124 115 60 61 -73 44 94 29 -118 92 83 -79 -99 -64 -27 -11 -
-46 127 -114 73 -103 75 8 71 82 -121 82 -88 -83 79 -104 -31 -78 73 -43 -96 -24 -125 -77 37 -69 110 -39 67 -112 -15 -86 107
32 78 -116 -114 -33 37 46 9 -87 47 -20 67 51 -72 74 61 -103 -16 -55 23 84 -2 -77 1 44 -12 83 -122 115 -117 -93 89 -107 -50
65 3 74 -44 -50 67 -109 -55 122 0 121 -21 97 -101 -118 -125 -95 -55 -13 -68 -128 -18 95 39 -60 -11 -64 -46 101 44 58 -48 79
105 48 -84 -110 51 87 -128 -68 -10 -126 -38 63 -54 -84 -67 115 126 45 24 37 -71 -5 100 26 92 -36 -70 -119 55 56 15 89 98 57
2 76 102 104 -73 51 100 25 -6 -127 -41 -94 -9 -32 3 29 -52 -126 112 -50 -25 -110 -87 4 -80 88 -113 -66 -22 -94 -111 -84 -66
7 45 47 75 111 -99 -85 18 -127 56 -4 56 -65 -119 -67 73 -125 62 -102 -53 -124 19 124 -101 -86 -39 -66 101 51 82 109 21 121
-116 90 122 11 -104 19 -59 -67 62 13 -21 25 78 -61 -98 -56 47 -38 -9 28 67 -127 61 58 13 -70 -92 -11 27 -96 -57 43 -113 12
-28 32 13 60 90 12 75 -18 -88 114 -118 94 -63 32 75 -93 109 68 0 44 -119 45 -26 7 2 -103 -90 -68 81 -68 59 63 76 -92 26 81
47 -106 106 -53 70 87 -71 -10 -82 -104 -87 -98 76 109 -88 -32 22 111 -46 31 -83 -15 123 110 -41 11 -48 107 85 52 31 107 -27
121 81 -30 110 127 23 -1 70 -110 -29 -122 -39 37 59 -98 -43 117 -117 42 45 122 -3 77 -119 32 92 -79 -37 11 95 -101 34 -26 -
4 -74 -70 110 57 -3 114 31 118 -76 -116 -42 73 -46 -106 -79 37 -55 -73 56 65 -13 -11 24 -122 -59 112 -124 -36 -92 28 100 10
8 124 23 -84 15 -39 -81 -13 -122 -70 -36 113 -82 -123 26 -77 -96 24 -60 20 -6 -21 34 -44 -97 -13 -59 -40 -45 114 -103 38 11
0 19 31 -25 -106 -82 -36 72 123 -85 112 103 -87 97 9 -90 49 -62 -121 -24 -30 -110 -19 -39 22 -8 48 14 -82 -78 44 118 -94 50
-87 38 12 116 -101 -54 53 78 -96 -123 26 13 110 52 81 1 -97 -8 -123 44 72 -98 -87 87 7 -126 -67 64 -42 -93 -113 -102 75 -2
103 -117 108 -16 87 -79 -59 89 18 -63 -70 -16 -128 26 -11 16 111 -40 -65 9 27 107 -83 32 -106 -123 -118 -119 -79 -112 -76 5
120 13 127 86 -125 -74 91 -88 -51 42 87 80 -27 49 22 -126 19 30 43 -106 7 -55 51 47 -63 -12 -77 -110 48 45 104 87 104 -51 -
-2 57 -96 -6 69 -32 62 -110 -106 28 24 -112 -121 -112 99 119 18 -48 -59 69 14 32 -20 70 13 70 98 -76 87 44 -77 53 36 97 7 -
-67 -37 -116 66 -89 91 65 -11 55 0 -96 -14 -35 111 7 -12 -14 32 -37 -44 64 -76 -20 33 -98 109 -44 42 -42 -108 -99 -36 18 90
-14 48 91 -4 -91 26 36 -76 76 44 -108 -57 24 24 -62 53 -91 33 15 -16 -117 26 -8 29 -18 100 117 -49 -17 107 -86 0 98 77 -51
```

6. CONCLUSION

This paper proposes a smart remote data backup technique. In this paper we have provided the algorithm for registration and authentication of user. It also explains cloud creation on central server which provides the facility to store user’s data. This paper provides the security to the user and user’s data is stored on central server by using RC6 block cipher algorithm. In future, we will create the back-up of same file on remote server to prevent data losses.

7. REFERENCES

[1] Ms. Kruti Sharma, Prof. Kavita R Singh, 2013, “Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing”, 2013 IEEE international conference on communication system and network technology, 6-8 April 2013, ISBN 978-1-4673-5603-9

[2] 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-1

[3] Kalyani Bangale, Nivedita Gupta, Swati Singh Parihar, "Remote Data Collection Server : E-Health Care" International Journal of Innovative Research in Computer and Communication Engineering, An ISO 3297: 2007 Certified Organization, Vol. 2, Issue 2, February 2014.

[4]Milind Mathur, Ayush Keasarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[5] Fouad Ramia, Hunar Qadir, "RC6 Implementation including key scheduling
using FPGA", ECE 646 Project, December 2006 [6] Boyang Wang, Baochun Li, Hui Li have presented a new technology "Oruta: Privacy-Preserving Public Auditing for Shared Data in Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, january-march 2014.

[7] S.Ezhil Arasu, B.Gowri, S.Ananthi presented "Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013.

[8] Giuseppe Pirr´o, Paolo Trunfio, Domenico Talia, Paolo Missier and Carole Goble, 2010, "ERGOT: A Semantic-based System for Service Discovery in Distributed Infrastructures," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

[9] Kruti Sharma, Kavita R Singh, "Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review" ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 5, November 2012

[10] Lili Sun, Jianwei An, Yang Yang, Ming Zeng, 2011, "Recovery Strategies for Service Composition in Dynamic Network," International Conference on Cloud and Service Computing.

[11] D. Srinivas, "Privacy-Preserving Public Auditing In Cloud Storage Security", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2691-2693.

[12] Tejashree Paigude, Prof. T. A. Chavan, "A survey on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Computer Trends and Technology- volume4Issue3-2013

[13] Ms Ruchira Titare, Prof. Pravin Kulurkar "Remote Data Back-up and privacy preserving Data Distribution in cloud: A review" International journal on computer science and mobile applications, vol

[14] Cong Wang, Qian Wang, and Kui Ren, "Ensuring Data Storage Security in Cloud Computing"