Securing Storage of Data in Cloud Computing

D. Dhayalan, S. Malcom
Department of MCA, Vel Tech Multi Tech Dr. RR and Dr. SR Engg College, Avadi, Chennai
Dayalan.moorthy@rediffmail.com, mali.math2010@gmail.com

Abstract-----*In this paper, a new data encoding scheme is proposed called layered interleaving. It provides good security. Thus, this extensive security and analysis of the performance shows that the proposed scheme is highly effective and efficient against Byzantine failure, the malicious data modification attacks, and server colluding attacks.*

Keywords: layered interleaving, Byzantine failure, Security, Recover.

1. INTRODUCTION:

The storage of data and information in Cloud has many challenges in designing that has been profound influence on the performance of the system. The biggest issue when storing data in Cloud is that the verification of data integrity at untrustedserver. The verifier's role has two categories: private access ability and public access ability. The private access ability scheme achieves high efficient, while the public access ability allows anyone, not only the data owner, to challenge the correctness of data storage when it has no private information in the server. The major concern in this scheme is secure and effective in dynamic operations on data blocks. Remotely stored data in the Cloud, not only can be accessed but also can be updated by the clients. The remote storage of data mainly focuses only on static data files, so there is a limitation in the dynamic data updates. The perspective of securing data which has always been an important in the quality of service, Cloud Computing gives number of reasons for it could not control the many new challenging security threats.

Firstly, the cryptographic method for data security protection cannot be directly used becausedue to huge loss of user's data and information in the Cloud. The Cloud conducts the Verification of correct data storage without explicit knowledge of whole data. The various kinds of data for each user not be given assurance in data safety for long term in Cloud Computing. Cloud becomes even more challenging in verifying data storage correctness.

Secondly, Cloud Computing is not just a data warehouse but also the user can update frequently the data which is stored in Cloud. It is important to ensure the correctness of data storage under dynamic data update.

Lastly, the redundant storage of individual user's data can be stored in multiple locations to reduce the data integrity threats. Therefore, distributed protocols used for storage correctness is the most important factor in achieving secure data storage in the Cloud.

2. Input Design And Output Design:

A. *Input Design:*

In input design there is a link between the user and the information system. The development and procedures are comprised for the preparation of data and to transact the data into a usable form, those steps are needed for processing which can be achieved to inspect the computer to read the data or information or allowing the user's to directly access the data in the system. The input design focuses to control the amount of input required, error controlling, avoid delays, avoids extra steps and keeps the process simple. The design of input provides security and easy use with retaining the privacy.

B. *Objectives:*

The process involved in designing the input is to convert a input of user-oriented description into a computer based system. This design is important to reduce the errors in the data input process and to give the correct way to the management to get the correct information from the design. It also describes how the information is used for immediate need and also for hard copy output.

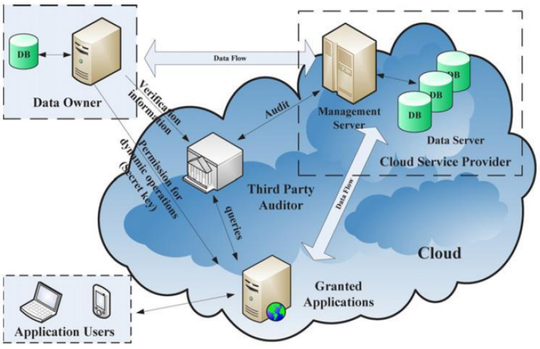
C. *Output Design:*

1. The output design is efficient to improve the relationship of system and help the user to make a decision. The right output needed to be developed when each output element is designed so that each user can recognize that the system can be used easily and effectively. When the computer analysis the output designs, it must be able to identify a particular output which will be needed to meet the requirements.
2. Methods are to be selected for presenting information.
3. Create documents or a report that contains information's produced by the system.

The form of the output of an information system should accomplish one or more of following objectives.

a) The information about the past activities and current status must be conveyed.
b) Actions are needed to be triggered.
c) Actions are needed to be confirmed.

3. System Architecture:



Audit system architecture for cloud computing.

Figure 1: Storage of Data in the Cloud

A. Existing System:

The perspective of securing data which has always been an important in the quality of service, Cloud Computing gives number of reasons for it could not control the many new challenging security threats.

Firstly, the cryptographic method for data security protection cannot be directly used because due to huge loss of user's data and information in the Cloud. The Cloud conducts the verification of correct data storage without explicit knowledge of whole data. The various kinds of data for each user cannot be given assurance in data safety for long term in Cloud Computing. Cloud becomes even more challenging in verifying data storage correctness.

Secondly, Cloud Computing is not just a data warehouse but also the user can update frequently the data which is stored in Cloud. It is important to ensure the correctness of data storage under dynamic data update.

Lastly, the redundant storage of individual user's data can be stored in multiple locations to reduce the data integrity threats. Therefore, distributed protocols used for storage correctness is the most important factor in achieving secure data storage in the Cloud.

B. Proposed System:

A new data encoding scheme is proposed called layered interleaving which is designed for time-sensitive packet recovery in the presence of huge loss of data. It has high-speed in recovering data, with minimum loss and forward error correction scheme is used to handle huge loss.

We must provide a pre-security in this cloud computing, while the malware detection occurs.

We must check and correct the user's data in the cloud by giving an effective and flexible distributed scheme with two features.

Homo-morphic token is utilized with distributed erasure-coded data for verification. This scheme achieves the integration of storage correctness and locates the data error, i.e., identifying the server's misbehavior.

The past idea has provided only the binary results about data storage across distributed servers. We propose a challenge response protocol in our work to locate the errors.

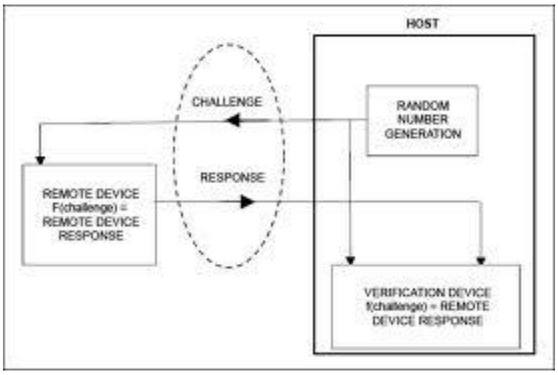

HOST
CHALLENGE
RANDOM NUMBER GENERATION
RESPONSE
REMOTE DEVICE F(challenge) = REMOTE DEVICE RESPONSE
VERIFICATION DEVICE f(challenge) = REMOTE DEVICE RESPONSE

Figure 2: Diagram of Challenge Response

This scheme is secure and efficient in dynamic operations on data blocks.

Thus, the extensive security and analysis of the performance shows that the proposed scheme is highly effective and efficient against Byzantine failure, the malicious data modification attacks, and also server colluding attacks.

4. System Study:

A. Feasibility study:

The proposed system is to carry out the feasibility during the analyses of system. This is to tell that the proposed system is not an overload to the company. In analyzing the feasibility, we should understand the major requirements of the system. Three things involved in feasibility analysis:

a) Economical Feasibility
b) Technical Feasibility
c) Social Feasibility

1. Economical Feasibility:

It will check the economic impact, in which the system will have on an organization. The fund that the company can pour for the research and developing the system is limited. We should justify the expenditure. Thus the system which is developed is within the budget and this is achieved by using free available of technologies. The customized product is only needed to be purchased.

2. Technical Feasibility:

It is needed to check the technical feasibility of the system. The technical resource must be available on high demand when system is developed. This will high demands being placed on the client. There should be new requirement while developing a system and no changes should be done for implementing the system.

3. Social Feasibility:

It is need to check the acceptance level of the system by user. The process includes the training of the user the use the system efficient and effective. The user should not be threatened by the system; instead it should accept the necessity of it. The methods involved in it are to see the level of acceptance by the user that is used to make a clear context about the system and to make him familiar with it. The confidence level of the user must raise and he must be able to make some constructive work.

5. Implementation:

A. Client Module:

Implementation is a stage when the theoretical explanations are converted into working system. It is the critical stage in achieving a successful new system and that gives the confidence to the user to search the related files in the database. At last, find the file and deliver it to the client.

B. System Module:

The representation of network architecture for data storage in Cloud is shown in Figure 1. There are three different network entities which can be identified as follows:

1. User:

Users who can able to store the data in the Cloud and can able to access the data from the cloud consist of both individual customers and organizations.

2. Cloud Service Provider (CSP):

A Cloud service provider, who has significant resources and has knowledge in building, and knows to manage distribute cloud storage servers and who owns and operate live Cloud Computing system.

3. Third Party Auditor (TPA):

The TPA who has knowledge and capabilities that the user may not also have can be trusted to access and elaborate about the risk in Cloud storage service on behalf of the user upon requests.

C. Cloud Data Storage Module:

In Cloud data storage, the user can able to store his data through cloud service provider into a group of cloud servers, which are simultaneously running, and user can able to interact with the cloud servers via cloud service provider to access and retrieve his/her data. Block level operation should be performed by user on his/her data. User has to protect his data with full security so that they continuously correct their stored data even if there is no existence of local copies. To monitor the data, user does not have resource and time feasibility, so that they can allow the task to the trusted third party auditor (TPA) of their own choice. In this model, an assumption of point-to-point communication channel is linked between each cloud server, so that the user can be authenticated and reliable.

D. Cloud Authentication Server:

Authentication server will add few additional behaviors to the client authentication protocol. Firstly, we have to send the client authentication information to the masquerading router. In this model, authentication server is also function like ticketing authority, which controls the permission on the application network. Authentication server supports other optional function to update the client list, cause a reduction in authentication time and checking the client as valid client depending upon the request.

E. Data Modification and Corruption are unauthorized:

The key issue in this model is to detect the unauthorized data modification and corruption. This happens due to server compromise and rand Byzantine failure. Modification of the data files is to prevent its original data when user retrieves the data.

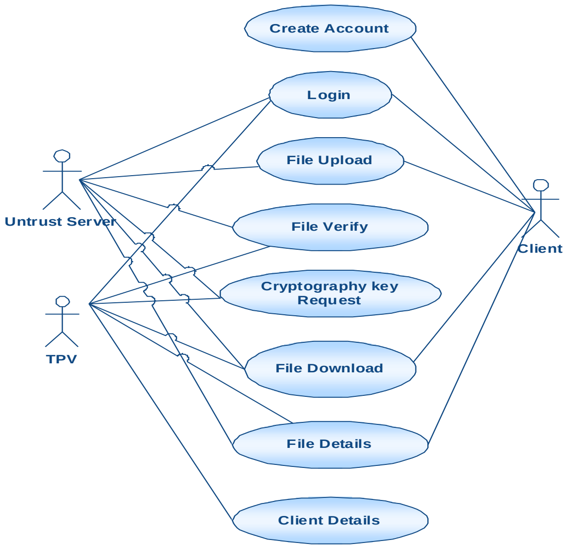


Figure 3: Driven model of Use case

6. Algorithm:

A. Pre- computation for token:

```
Parameter a, b and function c, d;
n is for token number
number n1 is chosen of indices per
  verification;
master key Kkey and challenge kchall is
  generated;
for vector V (j), j ← 1, n do
  for round i← 1, m do
    Derive i = fkchall (i) and kkey from Kkey.
    Compute Vi = k=1 ak ∗ G(j) [ck(i)(q)]ikey
  loop for is ended
loop for is ended
Vi is stored locally
```

B. Verifying the correctness and locating the error:

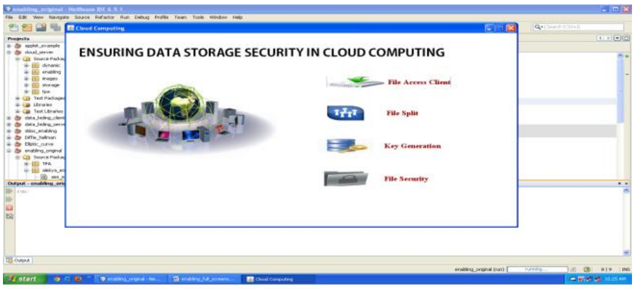
```
Re compute i = fkchall (i) and kkey from
  kkey;
Send {i , kkey } to the cloud servers;
rceve from servers:
  {Ri = r q ∗ G(j) [k (q)]|1 ≤ j ≤ n}q=1 ikey
for (j ← m + 1, n) do

  R(j) ← R(j) −  (fkj tsIq ,j )·q , q = k(i)
  (q)iq=1key
loop for is ended
Accept and ready for the further challenge.
if not
  server j is returning because of its
  misbehave
statement if is stopped
loop for is ended
statement if is stopped
finish
```

C. Recover the Error:

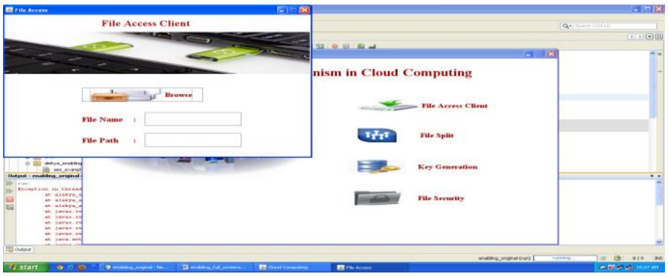
```
Corruption of block is assumed and
  have been detected.
r rows are specified;
% misbehaving server has been identified
  and assume s<k.
r rows are downloaded to avoid block from
  server;
s server is treated as erasure and block is
  recovered.
again send the recovered blocks to
  corresponding servers.
finish
```

7. Experimental Result:

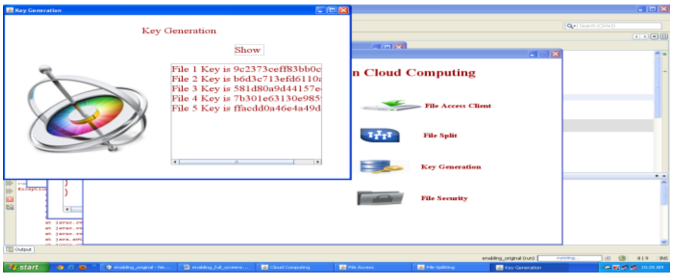
A. Data Storing in cloud:


enabling_original - NetBeans IDE 6.9.1
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Projects
Cloud Computing
ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING
File Access Client
File Split
Key Generation
File Security
Output
start

B. Login of client:



C. Authentication of server in cloud:



```
File 1 Key is 9c2373ceff83bb0c
File 2 Key is b6d3c713efd6110
File 3 Key is 581d80a9d44157e
File 4 Key is 7b301e63130e985
File 5 Key is ffacdd0a46e4a49d
```

8. CONCLUSION:

We discussed about the problem of securing data in cloud data storage, which is essential in distributed storage system. In proposed system, communication between user and cloud will reduce and storage of data will be secured. Finally, with our research on dynamic data storage in cloud, we also plan to check the problem of fine-grained data error localization.

REFERENCES:

i. *Amazon.com, Online at www.amazon.com*

ii. *N. Gohring, Amazon Online at www.pcworld.com*

iii. *Jules "PORs: Retrivievability proof, pg no:584-597.*

iv. *H. Sachem "Compact Proofs of retrieve ability", Asia Script procedure dec 2008.*

v. *K. D. Bowers, Retrievability proof, Report 2008/175eprint.iacr.org.*

vi. *G. Ateniese "Provable Data Possession at Untrusted Stores", pg no:598-611,2007.*

vii. *G. Ateniese "Scalable and Efficient Possessing Data ", pg no: 1-17, 2008.*

A. *Birrell "A Co-operative Internet procedure in Backup", pg no: 11, 2007.*

viii. *K. D. Bowers A High-Availability and Integrity Layer for storage in cloud", pg no:29-41, 2003.*

ix. *C.Wang, Q. Wang " Preserving public auditing for storage security in cloud computing" 10, March.2010.*