A Secure Cloud Peer-to-Peer Storage System Achieving Data Secrecy and Load Balance

Shin-Yan Chiou
Department of Electrical Engineering Chang Gung University, Tao-Yuan, Taiwan
ansel@mail.cgu.edu.tw

Abstract - Cloud technology is widely used for file sharing. Cloud systems have very desirable properties such as scalability, fault tolerance, and robustness. Several Cloud index structures have been proposed for equality queries, range queries, or other purposes. However, Cloud system is fraught with security risks and many security issues still exist in Cloud system. For solving these security issues, in our paper, we propose a secure and balanced storage system for Cloud system. The system offers load balance, secrecy, integrity, and robustness for data protection. It is efficient, reliant, and resilient. Moreover, the system is scalable.

Index Terms - Cloud networks, storage system, data secrecy, load balance, security

1. Introduction

Peer-to-peer (P2P) technology is widely used for file sharing. In the past decade a number of prototypes about P2P information retrieval systems have been developed. The appearance of data-sharing applications, such as Napster [1] and Gnutella [2], has made P2P systems popular for widespread exchange of resources and voluminous information between millions of users. P2P systems have very desirable properties such as scalability (from resource-sharing among cooperating peers), fault tolerance (as the symmetrical nature of peers), and robustness (due to self-reorganization after failures.)

Although P2P or cloud computing move the application and databases to the large data centres, the management of the data and services are not trustworthy. As the cloud services become popular [3], attackers may use cloud services to establish botnet and launch attacks. This attribute poses many security challenges [4][5].

In 2012, S.H. Lee and I.Y. Lee [6], [7] proposed a keyword searchable re-encryption scheme that let user share data with others safely by generating searchable encryption index. However, P2P system is still fraught with security risks [8] and many security issues still exist in P2P system. These issues [9] include (but not limited to) accessibility vulnerabilities, physical access issues, privacy and control issues arising from third parties having physical control of data, and issues related to data verification, tampering, integrity, confidentiality, data loss and theft.

For solving these security issues, in our paper, we propose a secure and balanced storage system for cloud P2P system. The system provide *balance ring*, which lets data stored in each nodes averagely. In addition, for data protection, it offers security properties including *secrecy*, *integrity*, and *robustness*. It prevents files from stealing, modifying, or destroying. Moreover, the system is *efficient*, *reliant*, *scalable*.

2. Proposed Method

The proposed system can be divided into four parts: (1) file preprocessing and data block indexing, (2) balance ring system management, (3) block distribution and retrieval, and (4) peer changing. In the system, two important tables, file index and node tables, are suggested putting on both the Client node and the other place. The file index/node table can be put on the Successor and Backer of ID(0)/ID(1). Table 1 defines the notations used in our proposed system.

A. File Preprocessing and Data Block Indexing

As shown in Figure 1 and Table 2, file preprocessing and data block indexing can be divided into two parts, (A) file encryption and segmentation, and (B) file composition, decryption and verification, where the details are described in [10].

Table 1. Notations

C	Ciphertext
$h(x)$	The hash value of x
I	$h(indx)$
$indx$	$h(c_1)\|\|h(c_2)\|\|h(c_3)\|\|\ldots\|\|h(c_k)$
l	The bit length of ID
M	Plaintext
N	The number of Peer nodes
N_m	The estimate maximum number of peer node
$\lceil x \rceil$	Ceiling function

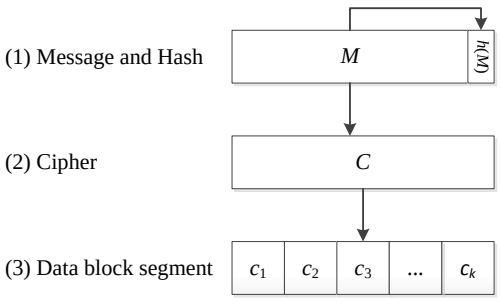

Fig. 1. File preprocess

Table 2. File Index Table

File Name	Time	Index
FN_1	t_1	I_1
FN_2	t_2	I_2
FN_3	t_3	I_3
FN_4	t_4	I_4

B. *Balance-Ring Management*

In this paper, we proposed a peer distribution method, called Balance Ring, where the most important point is the building of a Node Table, which records the information of each node's (A)ID, (B) IP or Domain Name, (C) Successor ID and (D) Backer ID. Each data will be stored in the Successor of each node. If needed, important data will be backup in the Backer of each node.

A physical peer occupies at least one peer node and is responsible for storing the blocks which are distributed to the peer node. The steps of building node table are shown as follows.

1) Decide the ID value

Before building node table, we have to obtain the number of peer node N or estimate the maximum number of peer node N_m. Take the value N or N_m to the pseudo-code in Figure 2 to decide the ID value of each node, where the bit length of node ID is $\lceil \log_2 N \rceil$ or $\lceil \log_2 N_m \rceil$. After that, fill in the value in the ID field of node table by the sequence of ID.

For example, assume $\lceil \log_2 N \rceil$ is 4. Take $\lceil \log_2 N \rceil = 4$ to the pseudo-code in Figure 2 and get the balance ring of Figure 3, where 0000(1) means that the node is the first node and its ID is 0000. It is recorded as ID(0) = 0000.

```
get_every_ID(N)
    ID(1) = 0;
    ID(2) = 1;
    for (j=1; j ≤ ⌈logN⌉-1; j++){
        for (i=2^j+1; i ≤ 2^(j+1); i++) {
            ID(i-2^j) = ID(i-2^j) *2;
            ID(i) = ID(i-2^j)+1;
        }
    }
```

Fig. 2. Obtaining the pseudo-code of ID

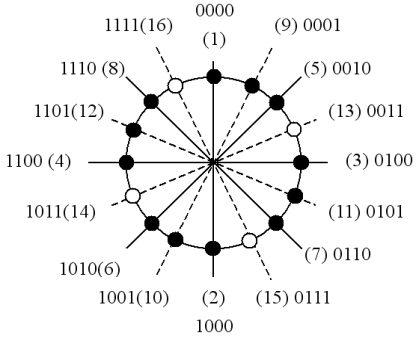

Fig. 3. Illustration of Balance Ring

2) Fill in IP or Domain Name (as shown in Table 3)

Fill in IP or Domain Name in the field IP(n) in node table by following the peer node number of each physical peer and the sequence n = 1, 2, 3, …. Fill in "Null" in the field IP(n) which does not fill in values.

For example (Table 3), assume there are 6 physical peers to store files. The first physical peer has four peer nodes and its ID is 163.97.25.33. Then Fill in 163.97.25.33 in the filed IP(n), where n = 1 ~ 4. Assume another five physical peer have (3, 2, 1, 1, 1) peer node separately and their IP are (61.219.38.220, 140.96.111.39, 239.27.74.104, 196.190.112.77, 209.59.137.56). We can fill in the corresponding IP value in the field IP(n), where n = 5 ~ 12.

Table 3. Node Table

n	ID(n)	IP(n) (IP or DN)	Successor ID	Backer ID
1	0000	163.97.25.33	0000	1110
9	0001	140.96.111.39	0001	0000
5	0010	61.219.38.220	0010	0001
13	0011	Null	0010	0001
3	0100	163.97.25.33	0100	0010
11	0101	196.190.112.77	0101	0100
7	0110	61.219.38.220	0110	0101
15	0111	Null	0110	0101
2	1000	163.97.25.33	1000	0110
10	1001	239.27.74.104	1001	1000
6	1010	61.219.38.220	1010	1001
14	1011	Null	1010	1001
4	1100	163.97.25.33	1100	1010
12	1101	209.59.137.56	1101	1100
8	1110	140.96.111.39	1110	1101
16	1111	Null	1110	1101

3) Successor ID

If a block is distributed to one node, the successor of the node is responsible for the block. The Successor ID of the node decides the storage address of the block. Of course, if there exist a peer node in one node and it is ready to store blocks, then the Successor ID of the node is the node itself. If there is not a peer node exist in one node, which means the filed IP of the node is Null, then the Successor ID of the node is the previous ID in which the field ID is not Null. (If we cannot find such node through the top of the node, we can find if from the bottom of the table.)

For example, in Table 3, the Successor ID of a node, in which the field IP is not Null, equals to the ID itself. The Successor ID of a node, in which the field IP is Null, equals to the previous ID. Also in Figure 3, the Successor ID of a black node, which stand for there is a peer in the node, equals to the ID itself. The Successor ID of a node, which stand for there is not a peer in the node, equals to the first black ID counterclockwise.

4) Backer ID

If a block is very important, it is needed to be duplicated to prevent the damage of the Physical Peer or the block. Then the block is needed to be duplicated to the Backer of the node. The Backer ID of a node equals to last ID of which the filed IP is neither Null nor the ID of its Successor IP.

For example, in Table 3, the Backer ID of the ID (0101, 1100, 1111) is (0100, 1010, 1110). As shown in Figure 3, the Backer of a black node *A* is the first counterclockwise black node *B* of which the IP is not that of node *A*.

The Note Table is very important and is suggested to be put on not only the Client node but also the Successor and Backer of ID(1). It can be encrypted if needed.

C. Block Distribution and Retrieval

If a file is going to be stored on our system, data blocks have to be distributed and stored in the Peer node after file encryption and segmentation. On the contrary, if a file is going to be retried from our system, data blocks have to be found from peer nodes and the file has to be synchronized, decrypted and verified after getting data blocks. The methods of block distribution and retrieval are described as follows.

1) Block distribution and storage

After file encryption and segmentation, we will get data blocks such as $\{h(c_i)||c_i\}$ and $\{I||indx\}$, where $h(c_i)$ and I are the index of blocks. Next, we take the former l bits of each block to map the ID of node table, where l is the bit length of an ID. Then, store each block on the Successor of the ID. If the block is important, it is duplicated on the Backer of the ID.

2) Block search and retrieval

If a file block is going to be retrieved, the file name and the file Index I have to be found form File Index Table. Next, take the former l bits of I to map the ID of node table. Then, use the Successor of the ID to fine data block $\{I||indx\}$. After that, use $indx = h(c_1)||h(c_2)||h(c_3)||\ldots||h(c_k)$ to get $h(c_i)$ and then use former l bits of $h(c_i)$ to map the ID in the Node Table. From the Successor the ID, $\{h(c_i)||c_i\}$ can be found. If a data block can not be found or an error is occurred, we can try to find the Backer of the mapped ID and check whether there is a duplicated block.

Besides, if a file is going to be deleted, the steps are the same as block search. After the block is found, delete the block directly and delete the file data from the File Index Table. If a file is going to be renewed, the action of "block search and retrieval" can be executed first. After the decision of file renewed, delete the old file and make the new file to execute the action of "block distribution and storage."

D. Peer Changing

After the decision of the number of Physical Peer (larger then 2) and the number of Peer Node, the system can be started to build. The peer node address of the system is not changed basically. However, the addition, departure and damage of peers will affect the peer node address. Then the node table has to be adjusted.

1) Peer join

"Peer join" means the client can store or retrieve data in the duration of adding peers. If a peer just adds and leaves, then there is not any influence for the system. The action of peer join is not needed.

There are two kinds of peer join. One is that the number of added peer node is not exceed the number of Null IP (i.e. IP = Null) in Node Table. Then the added peer node can be put on the place of Null IP. The other is that the number of added peer node is more than the content of the remained null place in peer node. Then the space of Node Table has to be increased and the ID bit length l has to be added. Generally, if the estimated peer node number N_m is correct, then this case will not happen.

(1) Case 1: The number of added Peer node is smaller than or equal to the number of Null IP:

In this case, the steps of peer addition are listed as follows. (Let SN_A denotes the added peer node.)

```
for (i = 1, i ≤ s ,i++) {
      n = 1;
      While (IP(n) ≠ Null) {n ++;}
      IP (n) = IP_A;
}
```

Fig. 4. The pseudo-code of adding Peer node

(a) Find the ID of added peer node

Let SN_A, IP_A and s denote the added peer node, the IP of SN_A and the added peer node number. Put s IP_A in the IP(n) that the value n is small, where n = 1, 2, 3, …. (For example in Table 3, put IP = 211.78.38.10 in IP (13).) The pseudo code of adding peer node is shown as Figure 4.

(b) Adjust the Successor ID and Backer ID of Node Table

The steps are listed as follows.

(i) Change the Successor ID of SN_A

Change the Successor ID of SN_A to the ID itself. For instance, Successor ID(13) = 0011.

(ii) Change the Successor ID of other nodes

Change the Successor ID of the entire white node (i.e. ID = Null) between the node SN_A and its first clockwise black node (i.e. ID ≠ Null) to the ID of SN_A.

(iii) Change the Backer ID of added peer nodes

Let BID_Z denotes the original Backer ID of SN_A. Change the Backer ID of SN_A to the ID of its first counterclockwise node of which the IP is neither Null nor the IP itself. For instance, Backer ID(13) = 0010.

(iv) Change the Backer ID of other nodes

Find node SN_A's first clockwise black node of which the IP is not the IP itself. Let the node ID be ID_B. Change the Backer ID BID_B of ID_B to ID_A. Change the Backer ID BID_Z of the entire ID_{Cv} between the black node ID_B and the node SN_A to BID_A, where v = 1, 2, 3, ….

(c) Store Successor blocks

After adding a physical peer and adjusting the Successor ID and Backer ID of Node Table, the entire added peer

nodes execute the following steps to store the responsible data blocks.

(i) Let n_A, ID_A, IP_A, SID_A and BID_A denote the value n, ID, IP, Peer ID and Backer ID of node SN_A. Record the entire white node ID between node SN_A and its first clockwise black node. Let ID_{Wu} denote the ID of the white node, u = 1, 2, 3, ….

(ii) From the node SN_A's first counterclockwise black node of which the IP is not IP_A, find the entire blocks that the former l bit of Index is ID_A or ID_{Wu}. Move them to the address of IP_A.

(d) Store Backer blocks

After adding a physical peer and adjusting the Successor ID and Backer ID of Node Table, the entire added peer nodes execute the following steps to store the responsible data blocks.

(i) From the data base of BID_Z, move the entire blocks that the former l bit of Index is ID_A or ID_{Cv} to BID_A, where v = 1, 2, 3, ….

(ii) From the data base of BID_B, move the entire blocks that the former l bit of Index is ID_B to ID_A.

(2) Case 2: The number of added Peer node is larger than the number of Null IP.

In this case, the steps of peer addition is the same as the steps in (1) except some steps of "note table extension and being renew." The steps are listed as follows.

(a) Increase the number and the bit number of ID

Take the bit length value l of the original ID to the pseudo code in Figure 5.

(b) Change the contents of Node Table

Double the value of Successor ID and Backer ID in Note Table. (i.e. Increase a bit "0" in the latter bit.) Let the IP value be Null in the added node and rearrange the Successor ID and Backer ID.

(c) Find the ID of added peer node (which is the same as (1)-(a))

(d) Adjust the Successor ID and Backer ID of Node Table (which is the same as (1)-(b))

(e) Store Successor blocks (which is the same as (1)-(c))

(f) Store Backer blocks (which is the same as (1)-(d))

```
Add_ID(l)
    l++;
    j = l – 1;
    for (i=2^j+1; i ≤ 2^(j+1); i++) {
        ID(i-2^j) = ID(i-2^j) *2;
        ID(i) = ID(i-2^j)+1;
    }
```

Fig. 5. The pseudo-code for increasing the number of ID

2) Peer leave

"Peer leave" means it will influence the host or handset of client to access data in the duration of adding departure. If a peer just leaves and joins, there is not any influence for the system and the action of peer leave is not needed. The steps of peer departure are listed as follows.

(1) Record the data of Successor ID and Backer ID

Let SN_L, (n_L, ID_L, IP_L, SID_L, BID_L), and ID_{sci}/ID_{bkj} denote the departure peer node, (the value n, ID, IP, Peer ID, Backer ID) of SN_L, and the node of which the Successor/Backer ID value is ID_L, i = 1, 2, 3, …, j = 1, 2, 3, ….

(2) Renew the Node Table

Change IP_L to Null. Renew all the Successor ID and Backer ID in Node Table.

(3) Backup the data of old peer Backer to new Backer

In the file peer BID_L, backup the entire block of which the Index point to ID_L and ID_{sci}, i = 1, 2, 3, … to the new Backer of BID_L.

(4) Move the Successor data

In the file peer IP_L, move the entire block of which the Index point to ID_L and ID_{sci}, i = 1, 2, 3, … to BID_L.

(5) Move the Backer data

In the file peer IP_L, move the entire block of which the Index point to ID_{bkj} to the new Backer of ID_{bkj}, j = 1, 2, 3, ….

3) Peer damage

"Peer damage" means a peer is unavailable or unrecoverable in the unexpected situation. If it can be known in advance or it is felt to be broken, the steps of Peer departure should be executed immediately. The steps of peer damage are listed as follows.

(1) Record the data of Successor ID and Backer ID

Let n_D, ID_D, IP_D, SID_D and BID_D denote the value n, ID, IP, Peer ID and Backer ID of the damaged peer node and ID_{sci}/ID_{bkj} stand for the node of which the Successor/ Backer ID value is ID_D, i = 1, 2, 3, …, j = 1, 2, 3, ….

(2) Renew the Node Table

Change IP_D to Null. Renew all the Successor ID and Backer ID in Node Table.

(3) Backup the data of old peer Backer to new Backer.

In the file peer BID_D, backup the entire block of which the Index point to ID_D and ID_{sci}, i = 1, 2, 3, … to the new Backer of BID_D.

(4) Backup the Backer data

In the peer node ID_{bkj} of which the IP is not Null, duplicate the entire (important) block of which the Index point to $ID_{bkj'}$, j' = 1, 2, 3, …to the new Backer of ID_{bkj}, j = 1, 2, 3, ….

3. Analysis of System and Security

A) System Scalability

In the system of balance ring, the ID length of each peer node is O(logN) (i.e. $\lceil \log_2 N \rceil$ or $\lceil \log_2 N_m \rceil$). The ID length of peer node occupies the minimum resource theoretically. If the physical peer is added so that the value N or N_m is needed to add, the ID length is still $\lceil \log_2 N \rceil$ or $\lceil \log_2 N_m \rceil$, which is still the minimum source theoretically. Hence when the physical peer adds, the system will not get much overload. Therefore the system is scalable.

B) System Security

In our system, we consider the security problem including the data privacy and integrity to prevent data being stolen, modified or destroyed. If a data is stolen, the attacker cannot obtain any information about the plaintext sine the data is encrypted. If the data is modified, file owners can detect the modification from the inconsistent hash value and, in advance, use the backup files. If attacker destroy or even delete a block, we can find the duplicated block from the backer of the block to get the destroyed or deleted block. Thus the system affords secrecy, integrity and robustness.

C) System Efficiency

In this system, we use only symmetric crypto system and one-way hash function. Compared with CFS, the speed of the whole system is promoted since the asymmetric crypto system is not used. Therefore, the system is efficient.

D) System Properties

The system is *reliant* because it can retrieve and redistribute all important data after a single peer suddenly terminating. It is also *resilient* since we can use any computer device to save our invaluable data by getting the backup data and retrieving all the files from nodes if our computer devices, such as PC or mobile phone, destroyed unexpectedly. Moreover, the system is *scalable* since it considers peer's join, leave, and damage.

4. Conclusion

For solving security issues for P2P Cloud system, we have presented a secure and balanced storage system. The system offers load balance, secrecy, integrity, and robustness for data protection. It is efficient, reliant, resilient and scalable. The security analysis and data collision are also discussed.

Acknowledgments

This work is partially supported by the NSC project under Grant NSC 102-2221-E-182 -038. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] Napster Inc., napster website, [Online]. Available: http://www.napster.com

[2] Gnutella, Gnutella website, [Online]. Available: http://www.gnutellaforums.com/

[3] D.Cenk Erdil, Simulating peer-to-peer cloud resource scheduling, Peer-to-Peer Networking and Applications, pp. 1-12, 2012.

[4] Wang C, Wang Q, Ren K., Ensuring data storage security in cloud computing, Cryptology ePrintArchive, Report [Online]. Available: http://eprint.iacr.org/, 2009.

[5] Jiang, H. and Shao, X., Detecting P2P botnets by discovering flow dependency in C&C traffic, Peer-to-Peer Networking and Applications, pp. 1-12, 2012.

[6] S.H. Lee and I.Y. Lee, Secure Index Management Scheme on Cloud Storage Environment. International Journal of Security and Its Applications, pp. 75-82, 2012.

[7] S.H. Lee and I.Y. Lee, Keyword Searchable Re-encryption Scheme Considering Cloud Storage-Service Environment. Information-An International Interdisciplinary Journal, pp. 2135-2146, 2012.

[8] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al., Security guidance for critical areas of focus in cloud computing, v2.1, Cloud Security Alliance, 2009.

[9] Subashini, S. and Kavitha, V., A survey on security issues in service delivery models of cloud computing}, Journal of Network and Computer Applications, Vol. 34, No. 1, pp. 1-11, 2011.

[10] S.Y. Chiou, "A Secure Cloud Saving System With Privacy, Integrity and Authenticity," International Conference on Business and Information 2012, Sapporo, Japan, July 7-9, 2012.