Distributed Challenge Response Mechanism for Error Localization in Cloud Computing

[1]V Sreeram, [2]K Senthil Kumar

[1]M.Tech Scholar, [2]Assistant Professor
SRM University
[1]sreeram_vempati@yahoo.com, [2]senthilkumar.k@ktr.srmuniv.ac.in

***Abstract* - Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications by using the concept of virtualization of resources. Though it provides various advantages, such a service also prone to several security issues as the data is outsourced, which leads to transparency of data, affecting the confidentiality. The outsourced data may be breached by unauthorized users who gain access to the data by breaching security levels of different servers where the information is stored. To provide security in this case encryption mechanisms are followed which reduces the dynamic data operations that can be applied over the encrypted data. To overcome this an approach which supports the use of homomorphic token generation and providing encryption at different stages of storing data in a remote system. And the auditing of data frequently for the purpose of integrity verification which can be achieved by validating the tokens generated along with the signature provided before outsourcing the data which helps in identifying the server which is being under attack or at risk.**

1. INTRODUCTION

The concept of the cloud has been around for a long time in many different incarnations in the business world .The cloud is a metaphor for the Internet. It refers the computers which are organised using a grid environment provided with a service oriented architecture.As cloud computing is growing in fame and the services offered by it also developing along with the globalization of the resources .

The security mechanism that are used in a single or a local system environment are considered in the initial stage of the development but the increase in knowledge and skills of the people are posing a threat and these traditional security measures are put through a test .Thus, there is a need for more secure and effective mechanisms to ensure the data is secure and integrity is verified. This gives the scope for the use of various techniques that are adopted to provide security and authenticity .The techniques available in earlier systems are much more of a single level security provision where traditional encryption and firewall techniques are provided to keep the information away from the untrusted parties. This situation alarms concern over the data security as many cloud service vendors are mainly effected due to the sever failures caused the malicious attacks which shows more measures are to be developed to achieve confidentiality, integrity of data outsourced.

Such a scenario leads to a situation where the data is corrupted in the server which is under attack and there is a need to retrieve original data by identifying the server location and then resolve the situation by collecting information about the data which is corrupted and replace it with the actual data.

Frequent monitoring of servers is to be done to identify their status which shows if any failure is detected.

2. PROPOSED SCHEME

The advent of cloud computing has increased the use of centralized locations in order to store the information and to make resources such as hardware ,services like operating system services and other application services are available without actually buying or setting up the infrastructure needed for them .They can be made use of from a centralized server or a cloud which provides these services to the local system that satisfies the credentials i.e. that are authenticated to make use of these services which provides the misuse of these centralized way of storage which make it easy for the untrusted parties to gain unauthorized access to data and manipulating the actual information which leads to integrity issues and some hackers may even try to damage the system with their method of adaptation to gain access to system which may lead to server failures .These issues are taken into consideration in the proposed design which consists of multi servers data distribution with distributed protocols implementation. Any server failing to use the cross server storage collect the data and provides quality data distribution to users or customers .This is called as a data dynamic support procedure .It can remove the redundant problems and increases the quality data distribution .In any server failure data identifies and recover from replication server. If any server shows any problems under distribution of data, the data can be recovered from another server .And the data from the server where the problem arised is collected and integrity checks are done identify if the integrity characteristics are satisfied by examining the data from that server with the actual data.

- It includes file splitting process, which means storing of data into multiple servers.
- This concept provides the users with the facility where the data stored in the cloud may not only accessed but also be frequently updated by the users.

- The splitted parts are encrypted where the homorphic token generated are embedded with the data in the split before storing it in different servers.

File Encryption

The files which are splitted are encrypted by making use of the encryption standards available which are combined with the hashed key value that is generated and then it is stored in the respective server over the cloud server environment.
The files can only be made available for access to the specified user who has the decryption key or the secret key.

HMAC code generation

1. function hmac (Key, message)
2. **If** (length(Key)> blocksize) **then** key=hask(Key)
3. **end if**
4. **If** (length(Key)< blocksize) **then** key=Key || [0x00 * (blocksize- length(Key)]
5. **end if**
6. o_Key_pad =[0x5c *blocksize] ⊕ Key
7. i_Key_pad =[0x36 *blocksize] ⊕ Key
8. **return**
9. hash (o_Key_pad || hash (i_Key_pad || message))
10. **end** function

File replicatiom

Once after the files are stored in their respective allocated servers their key values are also distributed along with data to the server where a copy of which it is maintained in the central server.

File Decryption

Unless and until the key generated with the padding provided during the encryption process which were limited only to the actual user the files cant be decrypted.

Encryption mechanism

The encryption process is done making use of the process of adding the padding bits with the actual data that is being encrypted.This provides an extra value or advantage of increasing the security.

Correctness Verification

The correctness verification and the error localization can be achieved by the following procedures .

Correctness verification and Error localization(CVER)

1. **procedure** CVER(I)
2. Recompute $\alpha_i = f_{kchal}(i)$ and $k^{(i)}_{prp}$ from K_{PRP};
3. Send $\{\alpha_i, k^{(i)}_{prp}\}$ to all the cloud servers;
4. Receive from servers:$\{R^{(j)}_{i=} \sum^{r}_{q=1} \alpha_i^q * G^{(j)}[\phi_k{}^{(i)}_{prp}(q)] | 1 \le j \le n\}$
5. **for**(j←m+1,n) **do**
6:$R^{(j)} - \sum^{r}_{q=1} f_{kj} S I_q, j) * \alpha_i^q, I_q = \varphi K^{(i)}_{prp}(q)$
7. **end for**
8.**if**$((R_i{}^{(1)}, \ldots\ldots R_i{}^{(n)}))$**then**
9. Accept and ready for the next challenge
10.**else**
11.**for**(j←1,n) **do**
12.**if**$(R_i^{(j)} != v_i^{(j)})$ **then**
13. **return** server j is misbehaving.
14.**end if**
15.**end for**
16.**end if**
17.**end procedure CVER**

3. SCENARIO

We present the scenario of the system where the data is stored over a distributed network of systems, improving the data confidentiality and integrity.

A. System Model

This system is designed for the identification of the misbehaving servers which may be caused due to the third party auditing mechanisms that allow the unauthorized users to make use of the information and may effect the working of the centralized system that may cause a system failure .The following are the steps followed for the purpose of achieving the mechanism for localizing the misbehaving servers.

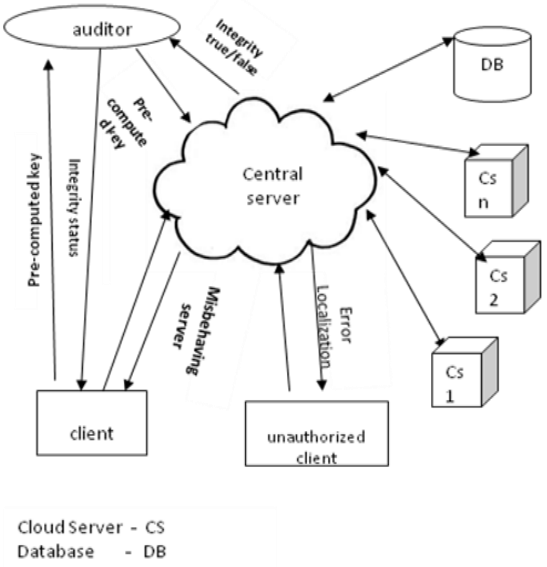

Fig 1:W orking model

1. Splitting up the data files or records: The actual files are splitted before encryption process takes place and are places in different servers. This method decreases the probability of gaining access to the actual data as it is stored at different location so that identification of the actual data can be hectic task as it is difficult to identify the entire data in their actual forms.
2. Encryption of the splitted files: The actual file which is splitted into different parts is encrypted along with HMAC code[1] which is generated which acts a token in order to verify the integrity of the data .And thus a cipher key is generated which is generated for each file after encryption which can be only provided to the authorized system or user.
3. Replication of files: The files or the data records have to replicated or stored in different systems or servers available in the cloud environment as a way to achieve the availability of data whenever required .As there might be a situation where a server or system is compromised and data might be corrupted .Thus, the replication process helps as data from other server or system can be used as it is not effected and the data from the central server can be used to identify the server failures by the process of integrity verification of data which is referred to as correctness verification.
4. Retrieval of actual data: The actual file that is splitted is requested the user who stored it in the cloud server which can provided to him by merging the splitted files back to its original form before that decryption process have to take place which makes use of the key value generated during the encryption process which is intended to a particular user who makes use of it to receive the data .And then, the files are merged back and integrity is put to verification, where the private key is used to decrypt the contents of the file .
5. Identification of misbehaving server: The data which is stored in different server in cloud environment is put through the above processes and at last the correctness verification of data is done which shows if there is any manipulation to the original data that is generated if not, the server is fine .Otherwise the server is compromised .This goes on with every system in the cloud network and thus the misbehaving servers are identified and necessary action are taken to provide higher level security to the system.

For error recovery:

1. procedure
   % Assume the block corruptions have been detected among
   % the specified r rows;
   % Assume s ≤ k servers have been identified misbehaving
2.Download r rows of blocks from servers;
3.Treat s servers as erasures and recover the blocks.
4.Resend the recovered blocks to corresponding servers.
5.end procedure

4. CONCLUSION

The process of providing the data security by encryption along with the provision of a pre-computed token which is used in the integrity or the correctness verification helps in the identification of the misbehaving or the compromised server in the cloud environment. The purpose is achieved with the generation of a signature in the form of MAC key generation. The keys that are used for decryption are provided only to the authorized users .Therefore the security of the centralized data is achieved which is important for the further growth of cloud computing.

REFERENCES

[1] S. Kamara and K. Lauter,"Cryptographic cloud storage," in RLCPS,2010.

[2] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (Crypto '96), pp. 1-15, 1996.

[3] Farhan Bashir Shaikh,Sajjad Haider, "Security Threats in Cloud Computing", 6th International conference on Internet technology and Secured transactions 2011.

[4] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008

[5] Amazon.com, "Amazon web services (aws)," Online at http://aws.amazon.com/, 2009.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[7] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud,"IEEE Internet Computing, vol. 16, no. 1, pp. 69

[8] M.A.Shah, R.Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, http://eprint.iacr.org, 2008.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores, "Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, Oct. 2007.