Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 3, March -2016

Carefree Data Access Solution for Public Cloud Storage

Mr. Akshay Ashok Suryawanshi[1], Mr. RohitHari Patil[2], Ms. Snehal Sunil Mane[3], Ms. AishwaryaDayanand Khanna[4]
Mr. RohitRajendra Jadhav[5]

[1-4]*Department of Computer Science and Engineering, Student at Sou. SushilaDanchandGhodawat Charitable trust's, Sanjay Ghodawat Group Of Institutions, Atigre, India.*
[5] *Department of Computer Science and Engineering, Student at Sou. SushilaDanchandGhodawat Charitable trust's, Sanjay Ghodawat Group Of Institutions, Atigre, India.*

Abstract: *The cloud computing paradigm is an impressive and interesting paradigm to the people in their trade and profession. Most of the people those who have their own occupation, trade or profession, are getting a great approach to the cloud computing standard. The attributes which are provided are simple and can be accessible to lead and organize. The cloud computing model has a right for an occupation with the chances of guaranteed means. The cloud storage allows the client to upload each of the functions that are present and it can be downloaded. Hence, the clients no longer hold theexpanded data, it is a dangerous project to maintain the data security in cloud storage paradigm.Theclient must not have any fear about the security of the data stored. The client can use the Third Party Auditor(TPA) whichchecks the integrity of the data and when the data is sent, the result is generated to the client. The Trust of the TPA is checked so that the cloud user doesnot have any fear of sending the request to an untrustedparty.*

Key Words: *TPA, AES, OTP, Integrity,CSP, etc.*

I. INTRODUCTION

The cloud is a collection of storage device, which consist of networks, hardware and interfaces. Cloud service provides dynamically scalable infrastructure of data file and storage.
Cloud computing works in different ways:

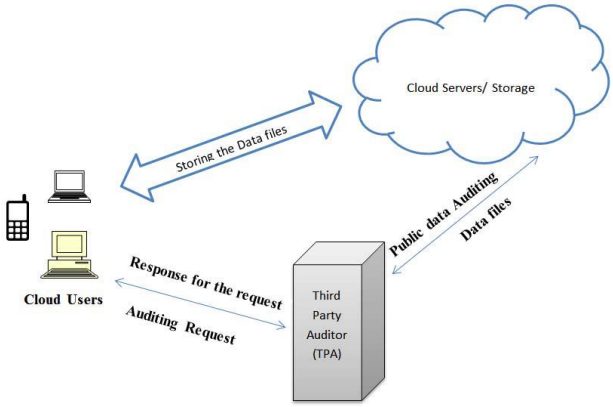
- Public clouds
- Private clouds,
- Hybrid clouds, which combines both properties of public and private.

- The cloud consists of various elements like end user, cloud service provider, Third Party auditor (TPA).
- The end user does not know anything about the ongoing technology
- The cloud service provider provides the services to the cloud user.

The client uses Third Party Auditor for verifying the correctness of the data files. It reduces the online burden of the cloud user and also reduces storage space.
The following features summarizes our contribution:
1. Auditing the data storage by using the external TPA, which is a server without learning the data content by using the privacy-preserving auditing protocol.
2. Batch auditing is done where multiple auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.
3. Providing data dynamics which are solved by using the version control system.
4. Ensuring the Third Party Auditor as the trusted person.

II. RELATED WORK

The basic technique is that the cloud user, who wants to store the data to the data center or cloud storage, it first generates the verification metadata for that file. The metadata is being sent to the Third Party Auditor in the parallel way the original data file is sent to the cloud storage through some secure channels. The cloud server then gets the data file along with the metadata and stores it in the cloud storage. The cloud user sends the request to the Third Party Auditor when it needs to retrieve data file. Upon the request from the user, the OTP that is a one time password is provided to the user. And then Third Party Auditor sends the request for getting the verified metadatathat is generated by the server as the same technique that the cloud user does. The verification data are sent to the Third Party Auditor from the data center, it then verifies the metadata received from the cloud user and the cloud server by comparing both. If both the data are same, the Third Party Auditor reports about the status of the users who requests for the file verification. If both the data differ, then report the cloud user about the updated data files.



The user after knowing the status of the file, they will retrieve the required file from the data center by entering the OTP which is generated. The integrity of the data is determined using the public auditing scheme.
This auditing scheme consists of two phases,

- Setup
- Audit

Following algorithms come under the public auditing schemes

- Keygen
- SigGen
- GenProof
- VerifyProof

Keygen is a key generation algorithm that is used by the clients to set up the scheme. The client generates verification metadata using the SigGen, which consist of digital signatures. The cloud server runs the GenProof to generate a proof of data storage correctness, whereas VerifyProof algorithm works withthe help of Third Party Auditor to verify the proof. Batch auditing is done by the Third Party Auditor (TPA) where multiple users send the request to the TPAand TPA processes the entire audit request at the same time.The auditoruses to keep track of both the current and previous tree roots generated by the user.The encryption and decryption of the data file and are done using the Advanced Encryption Standard (AES)algorithm[1].

III. PROPOSED SYSTEM

The client can retrieve the data file when the client verifies request.

The process involves these following terms:
1. Key tag: Key is generated to encrypt the file.

2. **Tag definition:** Single tag is generated for those files which are uploaded on a cloud at the same time.

3. **Sig Gen**: The checksum and the timestamp of the file which includes generation of the verification metadata

4. **Challenge**: Request which is sent is checked and proof of storage is generated.

5. **VerifyProof**: the metadata is compared and the file integrity is checked.

The new cloud user registers to the cloud server provider (CSP) before sending the file or before uploading the file to the cloud storage device. The registration of the new cloud user is done by the user name, password, mobile number and also by their email id which is required during registration. For highest security of the transferred data file the One Time Password (OTP) is generated. The user must have to login if he wants to upload the file onto the cloud. The files which are uploaded by the user or client are uploaded through some secure channels. The cloud service provider firstly verifies the user name and password, then only the file is uploaded. If there will be any fault in user name or password, then a message will be sent and the cloud user again asks to register to the cloud server. If once the cloud user uploads the data file which is received, the user encrypts that uploaded file using the algorithm that is encryption algorithm.For encryption and decryption the Advanced EncryptionStandard (AES) algorithm is usedwhere AES comprises three block ciphers[1]. Each cipher encrypts and decrypts data in blocks of 128 bitsusing cryptographic keys of 128, 192 and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192 or 256-bit key lengths. 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 include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.AES is more secure than its predecessors DES and 3DES as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES

The AES Algorithm have some features like:

- Block encryption implementation
- Symmetric algorithm requiring only one encryption and decryption key
- Data security for 20-30 years
- Worldwide access
- No royalties
- Easy overall implementation

AES ALGORITHM

Encryption Code:

```
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");  SecretKeySpec secretKey = new SecretKeySpec(key, "AES");
cipher.init(Cipher.ENCRYPT_MODE, secretKey);
String encryptedString = Base64.encodeBase64String(cipher.doFinal(strToEncrypt.getBytes()));
return encryptedString;
```

Decryption Code:

```
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");
SecretKeySpec secretKey = new SecretKeySpec(key, "AES");
cipher.init(Cipher.DECRYPT_MODE, secretKey);
String decryptedString = new String(cipher.doFinal(Base64.decodeBase64(strToDecrypt)));
return decryptedString;
```

The user must have to register to the Third Party Auditor which is created by the cloud user.Once the user registers to TPA, the metadata automatically send other details to it. The Homomorphic Tag Verification scheme, is generated in two phases :

- setup phase
- audit phase.

The user sends the data file to cloud server and that file which is sent is in encrypted manner. The cloud server stores the data file that is sent by user in the cloud storage device. Simultaneously, the Setup phase will be generated.

Setup phase includes two steps-

- Tag definition
- SigGen

When the data file is to be uploaded at the data center, over the same period of time, the file which is to be send is encrypted and then it is uploaded on cloud service provide(CSP).During upload mechanism the verification of the metadata is done by using SigGen Algorithm[2].The client when login to Third Party Auditor, by the name of file and user name the metadata is being sent. After sending data files and the verification the metadata is sent to the Cloud Server and Third Party Auditor.

The Audit phase includes two steps-

- Challenge
- VerifyProof.

When user needs to repossess the data file from storage space of cloud,the challenge step exist by sending retrieval request to Third Party Auditor[2]. Firstly the user enter the key value and obtain the details of each file from the database. Then the request goes to the TPA. The request consists of name of the user name of the file and information about the Cloud Service Provider(CSP). After receiving the request from the user, for receiving the file the TPA requests the CSP, the retrieval of the file is from data center,before retrieving the file the OTP is generated and is sent to the user. After receiving the OTP the user must enter that OTP to retrieve the uploaded files from CSP.And then the details are verified and is sent to TPA.

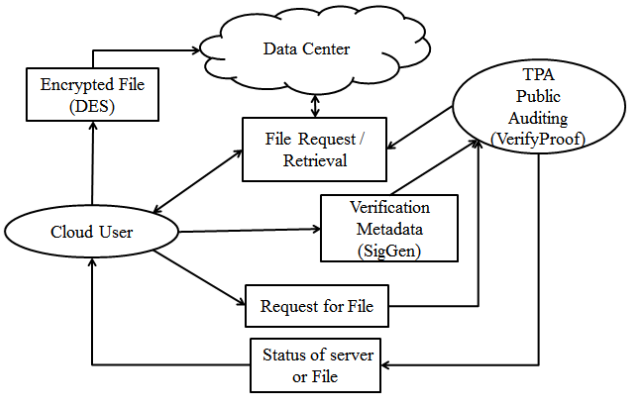


Figure: Overall System Architecture

Finally when TPA receives the file,the file storage proof is verified[2]. For the proof of the storage of file the VerifyProof step takes place by using VerifyProofAlgorithm[2]. After this the integrity of the file is verified and then TPA send the status of the file to the User.The user login to CSP and sends request for data file. The CSP, retrieve the file from the Data Center and send it to user.The status of the file which is sent by TPA is secured and the data integrity of the sent file is maintained.If the integrity of the file is not present then the error status message is being displayed to the user.The batch Auditing is done by the TPA. Batch Auditing is nothing but it checks or audit number of files at the same time. If user want a verification for multiple files,then user sends a verification request,then only the TPA return back all the data files at the same time through the data center.It also shows the storage proof of the data files.

IV. IMPLEMENTATION AND RESULTS

A. Document Encryption:

The data file which is sent is in encrypted form before uploading it to the cloud storage. Data fileis given as input. The file will be encrypted by the Advanced Encryption Standard Algorithm.

B. User Login:

If the user is already registered then the user can directly get login else the user must have to register.Each time the user must have to register or login accessing the data from cloud.By using name,password,email id and mobile number.

C. Cloud Drive:

Cloud Drive is an gateway for the cloud service. The uploaded data files are stored over the cloud drive where each user have separate user account. Each time the user have to login for storing or downloading the files from the cloud drive.The following figure shows the Own Cloud Drive where the data files are stored.

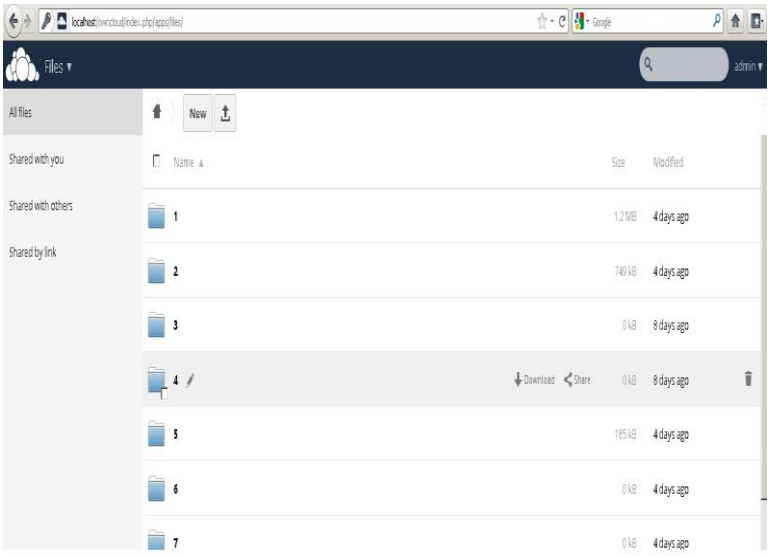


Figure:Own Cloud Drive

D. File Checking: The user sends the request to the TPA for the verification of file which includes the user name, password, file name and verification metadata.

E. File Decryption: The file which will be sent to the user will be in a decrypted form.The Decryption takes place by using AES Algorithm.

V. CONCLUSION

In our project we have developed several modules like User,Upload,Retrieve,Share. Our first module is User module with registration with his login session. In the second module we have implemented Upload module to store data file in encrypted manner. In Retrieve module when user tries to retrieve the file that time the user must enter the key that is (OTP) which is provided to his/her mobile number or email. The file is retrieved through TPA to the user and the retrieved file is in decrypted manner. The Retrieved file can also be shared by user to another user using the module called Share Module which we had developed in our project. In its future scope this can be done as Android application.

REFERENCES

[1]AES Algorithmhttp://techie-experience.blogspot.in/2012/10/encryption-and-decryption-using-aes.html

[2] P.Bharathi,S.Rajashree"Secure File Access Solution For Public Cloud Storage",2015.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in CloudComputing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no.5, pp. 847-859, May 2011.

[4] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services, "*IEEE Network Magazine*, vol. 24, no.4, pp. 19-24, July/Aug. 2010.

[5] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

