International Journal of Master of Engineering Research and Technology, 2394-6172-(O)
Volume-5, Issue-11, July 2018

DATA RETRIEVAL IN CLOUD STORAGE USING CLOUD AUDITING AND CRYPTOGRAPHY TECHNIQUE

Aadesh Dangi
Research Scholar M. Tech.
Computer Science & Engineering
Surabhi College of Engineering & Technology
Bhopal M.P. India
Dangiaadesh2@gmail.com

Mr. Rakesh Kumar Lodhi
Assistant Professor
Computer Science & Engineering
Surabhi College of Engineering & Technology
Bhopal M.P. India
Rakeshlodhi21@gmail.com

ABSTRACT

The security and authentication of data storage in cloud network is major issue. For the authentication and security of data used third party auditor. The third-party auditor authenticates the user and cloud service provider. The third-party auditor provides the authentication process of cloud data center to user level. The authentication of user and data center provide the facility of cloud data auditing. The cloud auditing of data used the process of proof of data retrieval. For the data retrieval over the cloud network. In the process of data auditing required security constraints for the integrity of data. for the integrity of data various authors used various cryptography technique symmetric and asymmetric. In this paper proposed cyclic key based data security technique for the integration of cloud data auditing. The proposed methods implement in ASP.NET with SQL server and used cryptography class for the application of crypto class. the performance of cyclic key is better than RSA cryptography technique.

Keywords: - Cloud Computing, security, integrity, TPA, Cyclic.

INTRODUCTION

Cloud computing is a computing technology, and the Internet has grown in recent years. It can share the soft-ware and hardware resources, and provide resources to a user's computer or mobile device. The user can obtain a more efficient service because cloud computing can integrate resources. Therefore, in order to achieve cloud computing technology, it must satisfy five basic features[1-2]: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service. However, is very difficult for general users or small and medium enterprises to construct cloud environment because they cannot afford the huge costs. There-fore, many information technology companies are finding business opportunities to cloud services. Thus, cloud service providers have joined to build cloud environments and provide services to the user. Cloud service providers offer three services including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Ser-vice (IaaS). The cost for users to rent cloud service is cheaper than the cost for users to build cloud environment[3-5].

Cloud storage service is the most common and popular service among many cloud services for general users[6]. Users have a bottleneck in local storage space because there are more and more users to save data in cloud storage, so cloud storage service has high capacity which solves users' difficult problem. Besides, cloud storage service provides high capacity space, and, in order to achieve ubiquitous service, it also provides to access cloud services from web service or applications that utilize the application programming interface (API) by mobile devices[7-8]. In the rest part of this paper, section II introduces data authentication & integrity, section III proposed model, section IV experimental work & result and finally section V discussed the conclusions.

II. DATA AUTHENTICATION & INTEGRITY

For the processing of data authentication of user and integrity of data design three phase model[9-11].

1. Admin section; - admin section deals with the user and TPA data authentication mechanism. The admin gives the whole ownership for the management of data security of user data. here admin play a role of ADMIN.
2. TPA: - third party auditor audits the user data with security constraints for the processing of submission of data and maintain the integrity of data. TPA also never change and edit the content of data over the cloud server.

Paper ID:- 2018/05/IJMERT/11/348

3. USER: - the user submits the data over the cloud server with authentication of key and download the data after verification of TPA.

Data encryption process[12-13]: The data encryption process is used in two mode in first mode user data are encrypted and send to admin and TPA. In second phase the data are encrypted to store cloud server and used the decryption for the key for data download.

Data Integrity[14-15]: The data integrity checks the content alteration by the user and TPA. If the content of data is modified by the TPA and some other user, further data cannot upload on cloud data server. For the validation of integrity used cyclic key generation technique.

III PROPOSED MODEL

REGISTRATION PHASE

This phase is responsible to register a UI with the ADMIN. This task can be achieved by using following set of operations.

1.1 Request for registration (UI →ADMIN):

IDADMIN || E(PRUI, IDUI || E(PUADMIN, (Ni ||Tj || "Request=NewReg")))

1.2 Registration acknowledged (ADMIN → UI):

E(PUUI, (IDUI || Ni || Tj || "Response=registered/ not registered"))

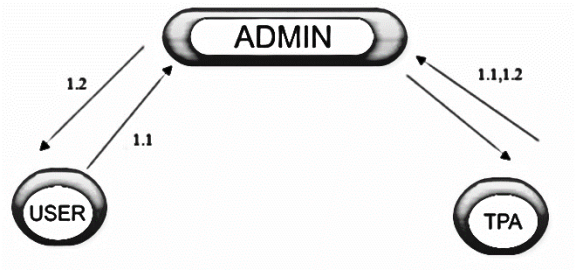

Figure 1: Registration Phase of user over cloud network.

During registration phase user send a registration request contain time stamp, ID of sender and this combined package is encrypted using a cyclic key of Sender. At the Cloud server it first decrypts the file using sender's cyclic key which give assurance that the sender is authenticate person and then the server decrypt the packet using its own private key and get the request's data. After processing Cloud server send an acknowledge back to the sender with status either Accepted or rejected by encrypting packet with cyclic key of receiver which is decrypted by private key of receiver and user check its request status from acknowledge. Here whatever information send the client is stored for future verification the table structure is shown below.

FILED NAME	:	FIELD DETAILS
User ID	:	ID of the user UI
Uname	:	User name
Password	:	Password of the user

2.1 Encrypt the file (Done by UI):

E(KF,F)

2.2 Calculate the Cyclic code & encrypt it (Done locally by UI):

HORG=E(KF, H(E(KF,F)))

This phase responsible to produce a secure data which can place on to the ADMIN. First, User encrypt the file which is available on local premises using and symmetric key. The key is produced by any of encryption schemes available. Once file encryption done the user calculate a hash code for the encrypted file. This hash code is generated using an encoding algorithm (e.g. SHA256, MD-5) Available. Client store the calculated hash into database for the future verification.

DATA DYNAMICS PHASE

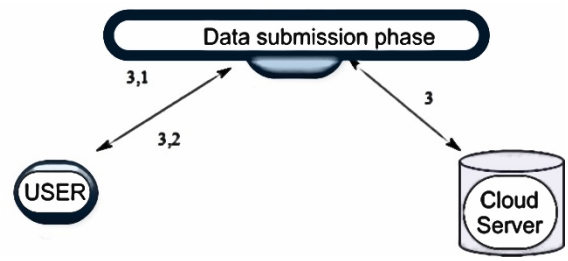

Figure 2: Data storage and data retrieval phase.

The main responsibility of this phase is to store the generated file in second phase is on ADMIN securely. This task in implemented using following set of operations

3.1 Request to store (UI → ADMIN):

C= IDUI || E(PRUI, IDUI || E(PUADMIN, E(KF,F) || Ni || Tj || HashType ||

equest=FileStore"))

3.2 Request to store confirmed (ADMIN → UI):

E(PUUI, (FileID || Receipt || Ni || Tk || "Response=Accepted/Rejected"))

During storage phase the client send "File Store" request to store the encrypted file with some more parameter like Sender's ID, Hash type Etc. by encrypting using cyclic key of ADMIN so only ADMIN can decrypt it and again encrypt same using private Now, At the ADMIN it decrypts the incoming coupon. First ADMIN decrypt coupon using cyclic key of sender and then again decrypt it using its own private key. It gets the data which it stores into the database and sends the confirmation to the senders by encrypting it using cyclic key of sender which contain status of request with the receipt. ADMIN maintain note of the files which is stored by different user on server into the database.

GRANT ACCESS RIGHTS PHASE

This is a one of the important phases of Model. During the phase the requested rights by the UI's are May granted or denied y the data owners. This task is implemented using some set of operations given below.

4.1 Grant access rights (UI → UI):

IDUI||E(PRUI, IDUI||E(PUUI, (FileID||AR||EncrType||HashType|| KF)))

4.2Make ADMIN aware (UI → ADMIN):

IDUI||E(PRUI, IDUI||E(PUADMIN, (FileID|| IDUI||AR)))

During Grant rights phase first Request sends by the requester on to the ADMIN which is stored by the server and intimate of the same to be given to Owner when owner makes check its pending rights. When owner finds a request for its file then either it grant or deny the grant request. In case of granting the request owner sends File ID, Hash type, Encryption algorithm used Etc. by encrypting with cyclic key of requester so that particular user can only decrypt it. Again owner encrypt the same using a private key of owner which gives surety to the receiver about authorization of requester. At the last the owner makes also aware to ADMIN about this by sending file Id, the user id whose request are fulfilled and the rights assigned Etc. encrypting by the cyclic key of ADMIN, and again use its own private key for encryption for the purpose of authentication. On the receiving this from the owner the ADMIN makes the necessary change into the database.

DATA DOWNLOAD PHASE

This phase contains the fundamentals for downloading a file from the ADMIN by the UI's.

The UI can only able to download the file from ADMIN if owner granted the rights for its

Request. This is achieved using following set of operations.

5.1 Request for data (UI → ADMIN):

IDuser||E(PRuser, Iduser || E(PUADMIN, (FileID || Ni || Tj || "DownloadReq")))

5.2 Data response (ADMIN → UI):

E(PUuser, E(KF, F) || Ni || Tj || "DownloadResponse=Accepted/Rejected"))

Once the user gets the permission from the owner the user can send the request to ADMIN for downloading of files. This request contains parameters like File ID, Time, ID of sender Etc. and whole request are encrypted using cyclic key of ADMIN, so only ADMIN can decrypt it. Again, the sender also encrypts same using its own private key which provides an authentication at the ADMIN side.

DATA VERIFICATION PHASE

This is the phase by which user can ensure about the correctness for him/his files. This phase contains following set of operations.

6.1 Data verification request (UI → ADMIN):

IDuser||E(PRuser, IDuser||E(PUADMIN, (FileID|| Ni || Tj || "VerifyReq")))

6.2 ADMIN computes the hash code & encrypts it:

HADMIN=E (PUuser, H (E(KF, F)))

6.3 Data verification response (ADMIN → UI):

E(PUuser, HADMIN || HORG || Ni || Tj))

During this phase the sender sends an verification request contains parameter like ID of file which they want to verify with the sender's ID by encrypting using cyclic key of ADMIN, so only ADMIN can decrypt it. Again this whole is encrypted using private key of sender so ADMIN can ensure that the sender is genuine. Once an ADMIN get the request it calculate the hash code for the requested file using an encoding scheme (Which is sent previously by owner) and encrypt it using an cyclic key of requester. This calculated reply is sent to the Requester where it is verified by the requester.

DATA UPDATE PHASE

This phase is responsible to update the existing file on to the ADMIN. This phase working in

somewhat same fundamental like in phase2.

7.1 Data update request (UI → ADMIN):

HORG=E(KF, H(E(KF,F)))

IDUI||E(PRUI, IDUI||E(PUADMIN, E(KF, F) || HORG || Ni || Ti || FileID))

7.2 Data update confirmation (ADMIN → UI):

E(PUUI, (Ni || Tj || FileID))

Once user gets the file from the ADMIN, user may make the changes into the file. Now this updated file must be store back to ADMIN so, for this first the user encrypt the file using shared symmetric key and calculate Hash of the updated file. Now user sends the request for updating file with the parameter like File ID, User ID Etc. by encrypting it using ADMIN's cyclic key so only it can access. Again sender encrypt it using a private key of sender so that ADMIN can authorize the sender and if sender is genuine then ADMIN update the database and makes mark about updating. After updating ADMIN sends confirmation to the user contain File ID and time by encrypting it using user's cyclic key.

IV EXPERIMENTAL WORK & RESULT

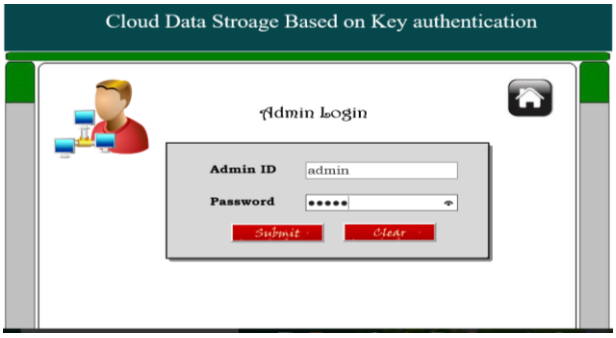

Figure 3: window show the admin window for enter login and password field with submit or clear button in our cloud data storage based on key authentication implementation.

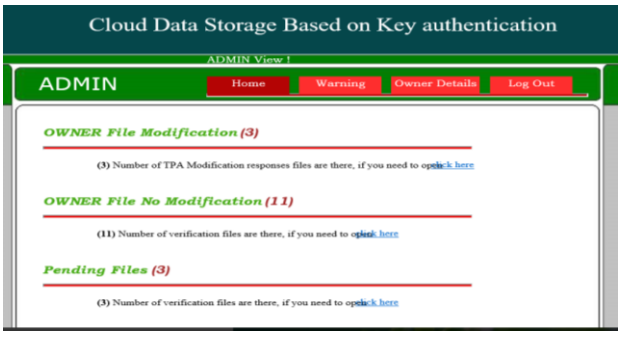

Figure 4: window show the admin window for enter login and password field and click on submit button in our cloud data storage based on key authentication implementation.

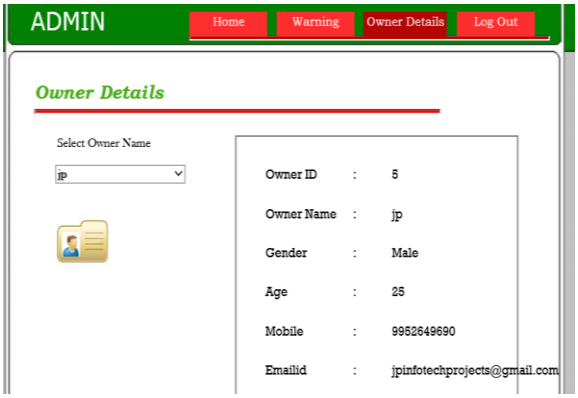

Figure 5: window show that owner button for select an owner button with dropdown list and see owner details in our cloud data storage based on key authentication implementation.

Types of File	File Name	Correct Key in %	Incorrect Key in %
Original File	math.txt	0.9	0.1
Fake file	physics.txt	0.85	0.15

Table 1: Shows that the comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the math and physics file.

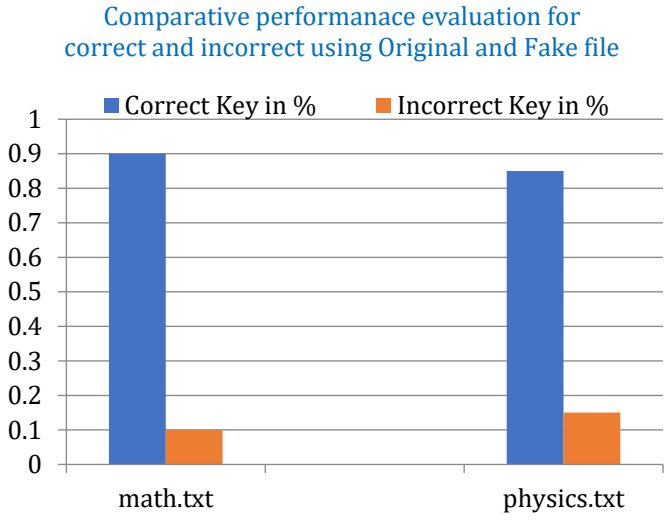

Figure 6: Shows that the comparative performance evaluation graph for original and fake files based on number of correct and incorrect in percentage value for the math and physics file.

Data size-text. file	RSA Method	Proposed Method
3	180	175
6	190	185
9	200	195
12	210	205
15	220	215
18	230	225
21	240	235
24	250	245
27	260	255
30	270	265

Table 2: Shows that the comparative performance for Computation time on the basis of data size using methods RSA and Proposed with text. file.

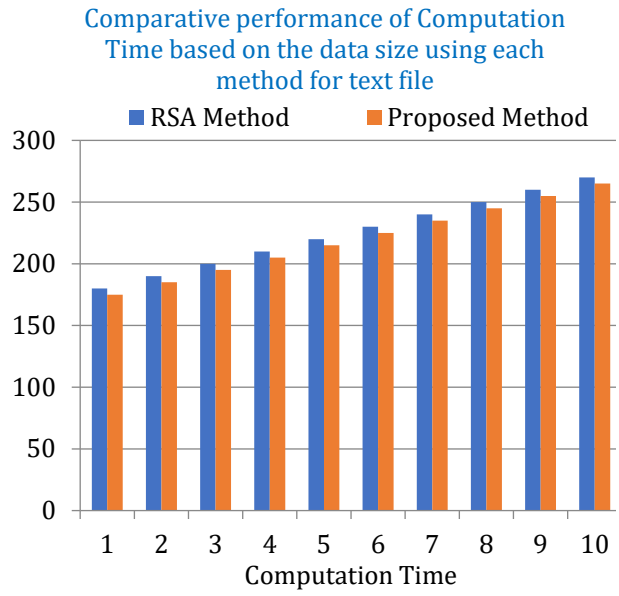

Figure 7: Shows that the comparative performance for Computation time on the basis of data size using each method like, RSA and Proposed with text file, here we find the value of computation time for respectively data size and methods.

V CONCLUSION

Privacy and data Security responsibilities within the cloud should be a collaborative effort between both service providers and users. These responsibilities differ by the kind of cloud services been consumed. The cloud service provides is on duty to ensure the security of cloud data storage and to ensure maximum protection. Service providers have the responsibility to ensure the public data integrity and isolation protections are put in place to mitigate the risks users pose to one another in terms of data loss, misuse, or privacy violation within the cloud. Again, from the cloud service provider's perspective, there should be an active monitoring mechanism in place to allow for effective planning and implementation of services. This also serves as a means to respond to events quickly and more efficiently. Cloud users on the other hand must ask and be clear about their responsibility for their security. By this, it is recommended to SMEs to ask question about their security when engaging a service provider. Questions about; what information is stored on a system, where is the information stored, who can access the system, what they can access and appropriate access mechanism are good to clear any doubt about services providers. Identifying controls that address the lack of direct access to data and information is the foundation of SME's strategy for entering the cloud and allows the organization to consistently approach security needs based on the workloads and granular data represented in their cloud efforts.

REFERENCES

[1] Jin Li, Xiao Tan, Xiaofeng Chen, Duncan S. Wong, FatosXhafa, "OPOR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices" IEEE 2015, Pp 195 205

[2] Keke Gai, Meikang Qiu and Hui Zhao "Cost-Aware Multimedia Data Allocation for Heterogeneous Memory Using Genetic Algorithm in Cloud Computing", IEEE, 2016, Pp 1-6.

[3] Wei-Fu Hsien, Chou-Chen Yang and Min-Shiang Hwang "A Survey of Public Auditing for Secure Data Storage in Cloud Computing", International Journal of Network Security, 2013, Pp 133-142.

[4] Prof. N.L. Chourasiya, DayanandLature, Arun Kumavat, Vipul Kalaskar, Sanket Thaware."Privacy-Preserving Public Auditing for Secure Cloud Storage" International Journal of Engineering Research and General Science, 2015, Pp 744 -748.

[5] Chi-Wei Liu, Wei-Fu Hsien, Chou-Chen Yang and Min-Shiang Hwang "A Survey of Public Auditing for Shared Data Storage with User Revocation in Cloud Computing", International Journal of Network Security, 2016, Pp 650-666.

[6] K. Sujatha and K.Sundar "A Survey on Integrity Verification in Cloud Computing", IJSRD, 2015, Pp 209-213.

[7] PradnyaChikhale, NamrataDwivedi, ParnaDutta, AparajitaSain, VrundaBhusari"Enhancing Data Storage Security In Cloud Computing Using PDDS Technique" PISER 2014 Pp 53-59.

[8] Shubham Nema, Akash Mittal and Yogendra Kumar Jain "Proof of Retrievability in Cloud Computing Environment using Sharing of Key based on Resource", International Journal of Computer Applications, 2016, Pp 1-6.

[9] Shalini J and Dr. K. Raghuveer "Efficient Implementation of Proof of Retrievability (OPOR) In Cloud Computing with Resource Constrained Devices", Int. Journal of Engineering Research and Applications, 2016, Pp 62-67.

[10] Betzy K. Thomas, M. NewlinRajkumar "A Dynamic Public Auditing SecurityScheme To Preserve Privacy in Cloud Storage" IJSHJE 2013, Pp 93-97.

[11] Ujjwala Bandawane and Sandeep Gore "Survey on Evidence of Retrievability Schemes of Cloud Storage Services for Resource-Strained Devices", IJSR, 2013, Pp 1394-1398.

[12] Maddipatla Sailaja, Varaprasad Gajjala and Karamala Suresh "Enabling Proof of Retrievability in Cloud Computing with Resource Constrained Devices", IJITECH, 2016, Pp 902-907.

[13] K.Anuja and A.Nirmal Kumar "A Survey On Outsourced Proof Of Retrievability In Cloud Computing", Journal Of Applied Sciences Research, 2015, Pp 10-13.

[14] C. Sarika and R. Megiba Jasmine "an outsourced proof of retrievability for dynamic data operation in cloud", IJRSET, 2013, Pp 19-22.

[15] HarleenKaur, Er. VinayGautam "A Survey of Various Cloud Simulators" International Journal of Computer Sciences and Engineering 2014 Pp35- 38.