Proof of Retrievability in Cloud Computing Environment using Sharing of Key based on Resource

Shubham Nema
Computer Science and Engineering Dept.
SATI
Vidisha, India

Akash Mittal
Computer Science and Engineering Dept.
SATI
Vidisha,India

Yogendra Kumar Jain
Computer Science and Engineering Dept.
SATI
Vidisha,India

ABSTRACT

The storage and retrieval of data over cloud computing is big issue. For the storage and retrieval cloud computing used the concept of authentication and authorization. The process of authentication and authorization used primary and secondary authentication system. In primary authentication system used login id and password, in secondary login used the OTP and some other verification code. In both login systems trap the OTP code and primary information of user and the security process of cloud environment are compromised. In this paper proposed a model of secured access based on the concept of fake and genuine user. In the case of fake user the received file is fake. This file is generated by the system. For the authentication of genuine and fake user used the concept of shared key concept. The shared key gives the option of retrieval of data over cloud environment. The proposed model implemented in java software and used java RMI tool for access of remote machine.

General Terms

Cloud Computing, Data Dynamics, Proof of Retrievability.

Keywords

Authentication, cryptography, Sharing of Key.

1. INTRODUCTION

Cloud computing environment gives a highway of data storage and retrieval of data over network. The major concern in cloud computing environment is authentication and authorization of user. The cloud environment gives the primary and secondary authentication system based on login id and password. Now a day's various hacker and cracker trap the primary information of user data and retrieve cloud data. In concern of security issue cloud network faced a various types of threats[1,2]. For the controlling of damage various security and access control model are used. The cloud computing gives the concept of data dynamics for the updating and deletion of data over the cloud network[3,4]. In data dynamics the cloud network faced a problem of proof of retrievability. The proof of retrieval ensue the genuine user and fake user. In case of fake user the proof of retrieval gives the duplication and another data to fake user as a normal and genuine user. For the proof of retrieval various access control and security model are used. In consequence of security model used cloud service server and third party auditor[5,6,7]. The third party auditor audits the load data on data storage server. The role of TPA improves the security strength of cloud over data. In this paper design a model for the proof of retrievability over cloud computing scenario. The proposed model used the concept of shared key. The concept of shared key depends of generation of cloud server key and TPA key. The generation fashion of key based on randomized algorithm. the randomized algorithm generates the share key for the authentication and authorization of user. It take three time user code for the process of authentication. If the key value is matched the user enters the process of retrieval and if key value is not matched the user access the data as fake user. The concept of fake user supports the validation process for the retrieval of data[8.9.10]. The retrieval of fake data measures the hit count of access level and block the account of user for further validation. This paper is divided into five sections. Section-1. Gives the introduction proof of retrieval. Section-2. Shared key generation . Proposed method in section-3.. In section-4. Discuss experimental work and finally discuss conclusion and future work in section 5.

2. SHARED KEY GENERATION

The concept of shared key generation based on the randomized algorithm the sharing of key depends on the information transformation of cloud service server and cloud service provider. The cloud server provider involved the third party auditor for the authentication process. The key generation process involved the TPA and cloud service server.

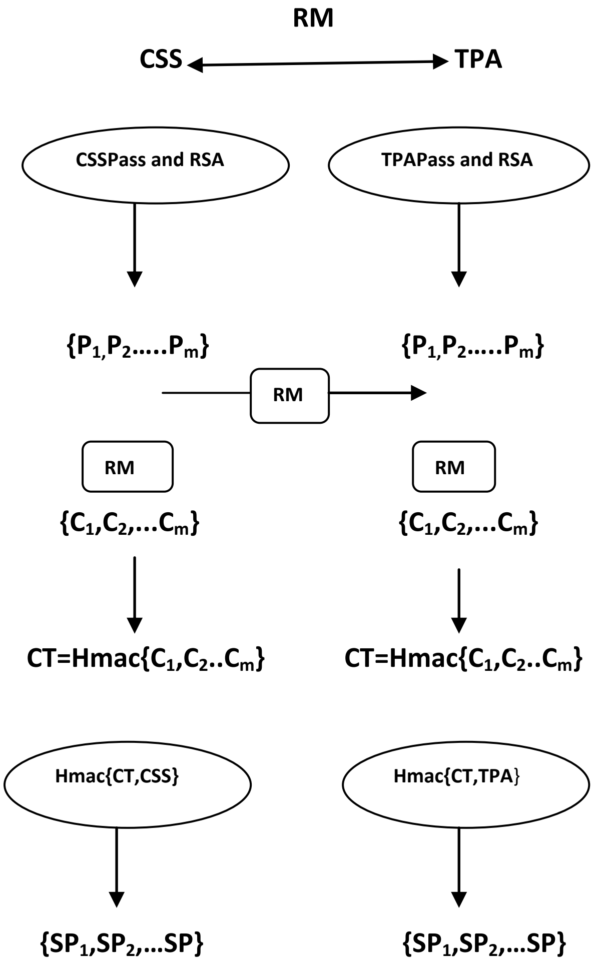
RM
CSS
TPA
CSSPass and RSA
TPAPass and RSA
$\{P_1, P_2 \ldots\ldots P_m\}$
$\{P_1, P_2 \ldots\ldots P_m\}$
RM
RM
RM
$\{C_1, C_2, \ldots C_m\}$
$\{C_1, C_2, \ldots C_m\}$
$CT = Hmac\{C_1, C_2 .. C_m\}$
$CT = Hmac\{C_1, C_2 .. C_m\}$
Hmac{CT,CSS}
Hmac{CT,TPA}
$\{SP_1, SP_2, \ldots SP\}$
$\{SP_1, SP_2, \ldots SP\}$

Figure 1: Shows shared key generation technique

3. PROPOSED METHODOLOGY

The proposed model used five phase for the authentication of user. The authentication of user provides the proof of data retrieval for the accessing. The process of model describe as.

1. Registration Phase:

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

1.1 Request for registration (UI →CSP):
IDCSP || E(PRUI, IDUI || E(PUCSP, (Ni ||Tj || “Request=NewReg”)))

1.2 Registration acknowledged (CSP → UI): E(PUUI, (IDUI || Ni || Tj || “Response=Accepted/Rejected”))

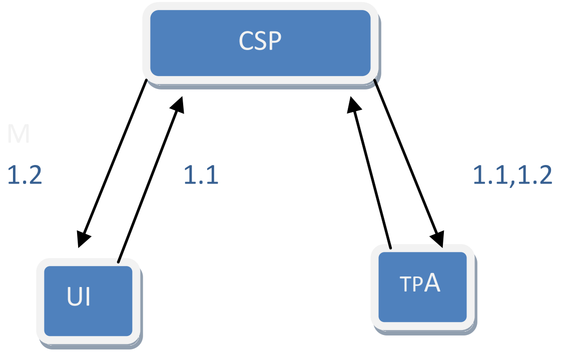

Figure 2 : Registration Phase of user over cloud network

During registration phase user send an registration request contain time stamp, ID of sender and this combined package is encrypted using an cyclic key of Sender. At the Cloud server it first decrypt 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.

FieldName	Field Details
UserID	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 CSP. 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.

3. Data dynamics phase

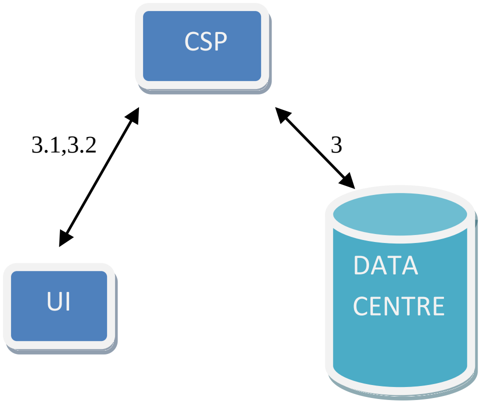

Figure 3: Data storage and data retrieval phase

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

3.1 Request to store (UI → CSP)
C= IDUI || E(PRUI, IDUI || E(PUCSP, E(KF,F) || Ni || Tj || HashType || Request=FileStore"))

3.2 Request to store confirmed (CSP → 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 CSP so only CSP can decrypt it and again encrypt same using private Now, At the CSP it decrypts the incoming coupon. First CSP decrypt coupon using cyclic key of sender and then again decrypt it using its own private key. It gets the data which it store 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.CSP maintain note of the files which is stored by different user on server into the database.

4. Grant Access Rights Phase:
This is a one of the important phase 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)))

4.2 Make CSP aware (UI → CSP):
IDUI||E(PRUI, IDUI||E(PUCSP, (FileID|| IDUI||AR)))
During Grant rights phase first Request sends by the requester on to the CSP 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 CSP about this by sending file Id, the user id whose request are fulfilled and the rights assigned Etc. encrypting by the cyclic key of CSP, and again use its own private key for encryption for the purpose of authentication. On the receiving this from the owner the CSP makes the necessary change into the database.

5. Data Download Phase:

This phase contain the fundamentals for downloading a file from the CSP by the UI's.

The UI can only able to download the file from CSP if owner granted the rights for its Request. This is achieved using following set of operations.

5.1 Request for data (UI → CSP):

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

5.2 Data response (CSP → 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 CSP for downloading of files. This request contain parameters like File ID, Time, ID of sender Etc. and whole request are encrypted using cyclic key of CSP, So only CSP can decrypt it. Again the sender also encrypts same using its own private key which provides an authentication at the CSP side.

6. Data Verification Phase:

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

6.1 Data verification request (UI → CSP):

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

6.2 CSP computes the hash code & encrypts it:

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

6.3 Data verification response (CSP → UI):

E(PUuser, HCSP || 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 CSP, so only CSP can decrypt it. Again this whole is encrypted using private key of sender so CSP can ensure that the sender is genuine. Once an CSP 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.

7. Data Update Phase

This phase is responsible to update the existing file on to the CSP. This phase working in somewhat same fundamental like in phase2.

7.1 Data update request (UI → CSP):

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

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

7.2 Data update confirmation (CSP → UI):

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

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

4. EXPERIMENTAL RESULT

The proposed model implemented in java software and used Google cloud interface for the storage of data. For the remote access of data used the concept of RMI tools. For the validation of model generates logs of fake user and genuine user. The stored log gives the information of fake user and genuine user[16].

Table1: Shows that the comparative performance for Computation time on the basis of block size using methods DRDP, RSA Based and Shared Key Based.

DRDP Method		RSA Based Instantiation		Shared key Based	
Block Data size	Computation Time	Block Data size	Computation Time	Block Data size	Computation Time
0	200	0	220	0	210
20	220	20	240	20	230
40	240	40	260	40	250
60	260	60	280	60	270
80	280	80	300	80	290
100	300	100	320	100	310
120	320	120	340	120	330
140	340	140	360	140	350
160	360	160	380	160	370
180	380	180	400	180	390

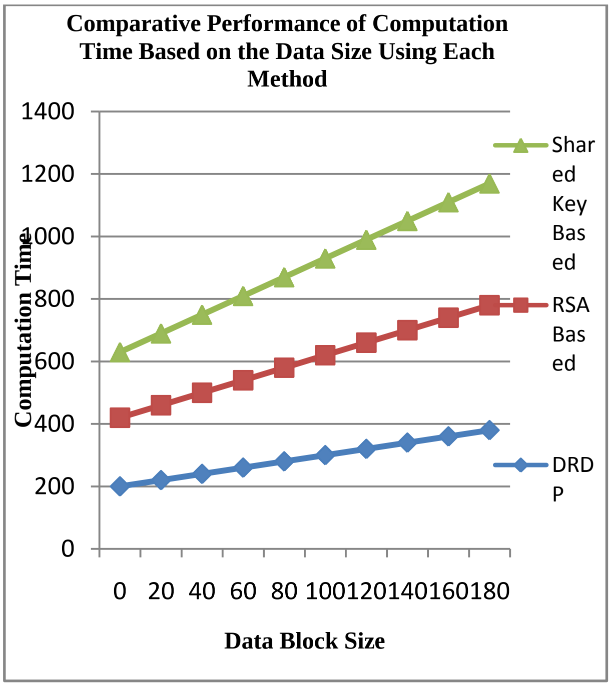

Figure: 4 Shows that the comparative performance for Computation time on the basis of data block size using each method like DRDP, RSA Based and Shared Key Based, here we find the value of computation time for respectively block size and methods.

5. CONCLUSION AND FUTURE WORK

In this paper proposed a model of proof of rerievability based on the concept of shared key generation. The process of shared key generation used two different part CSS and TPA. The CSA and TPA used the randomized key generation technique for the processing of user authentication. The proposed model validate the genuine and fake user. For the minimization of attack possibility the CSS server automatic generates fake file for unauthorized user. The fake user accept the fake file and not hit the sever next time and save the computational time of server. The proposed model validate in RMI server for remote machine and also validate the key generation process technique. Our experimental result shows better performance instead of pervious algorithm for proof of retrievability.

6. REFERENCES

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

[2] Qian Wang, Kui Ren, Member, Wenjing Lou, Jin "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE 2011 847 - 859

[3] Meera Chheda, Anmol Achhra, Priyanka Vaswani, Rajeshwari Agale, Vidya Bhise. "Public Auditing For The Shared Data In The Cloud". International Journal of Advance Foundation and Research in Computer (IJAFRC) 2015 Pp 724-728.

[4] Prof. N.L. Chourasiya, Dayanand Lature, 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] R.Guruprasath, M.Arulprakash "Privacy Preserving Public Auditing For Shared Data With Large Groups In The Cloud" Journal of Recent Research in Engineering and Technology 2015 Pp 40-46

[6] Mrunali Pingale, Prof. Jyoti Pingalkar "Security Preserving Access Control Mechanism In Public Clouds Using PANDA Security Mechanism" iPGCON, 2015 Pp 1-5.

[7] Pradnya Chikhale, Namrata Dwivedi, Parna Dutta, Aparajita Sain, Vrunda Bhusari "Enhancing Data Storage Security In Cloud Computing Using PDDS Technique" PISER 2014 Pp 53-59.

[8] J.Aparna, Mr.R.Sathiyaraj "Auditing Mechanisms for Outsourced Cloud Storage" International Journal of Computer Science and Mobile Computing, 2014, Pp 219-229

[9] Ch. Rajeshwari, S. Suresh "An Efficient PDP Scheme For Distributed Cloud Storage To Support Dynamic Scalability On Multiple Storage Servers" International Journal of Science Engineering and Advance Technology, 2014 Pp 985-988

[10] Betzy K. Thomas, M. Newlin Rajkumar "A Dynamic Public Auditing Security Scheme To Preserve Privacy In Cloud Storage" IJSHJE 2013 Pp 93-97.

[11] GuangyangYang, Hui Xia, Wenting Shen, Xiu xiu Jiang,Jia Yu "Public Data Auditing with Constrained Auditing Number for Cloud Storage" 2015 IJSIA Pp 21-32.

[12] Jian Yang, Haihang Wang, Jian Wang, Chengxiang Tan , Dingguo "Provable Data Possession of Resource-constrained Mobile Devices in Cloud Computing" Journal Of Networks, 2011 Pp1033-1040.

[13] Javed Akthar Khan, Ritika Arora "A Review of Cloud Environment and Recognition of Highly Secure Public Data Verification Architecture using Secure Public Verifier Auditor" International Journal of Electrical, Electronics and Computer Engineering 2014 Pp144-148.

[14] Harleen Kaur, Er. Vinay Gautam "A Survey of Various Cloud Simulators" International Journal of Computer Sciences and Engineering 2014 Pp35- 38.

[15] Clementine Gritti, Willy Susilo, Thomas Plantard ,Rongmao Chen "Improvements on Efficient Dynamic Provable Data Possession scheme with Public Veri_ability and Data Privacy"Centre for Computer and Information Security Research 2014 Pp 1-19

[16] Chunming Gao, Noriyuki Iwane "A Social Network Model With Privacy Preserving And Reliability Assurance And Its Applications In Health Care " International Journal Of Energy, Information And Communications 2015, Pp.45-58.