A SECURED ENCRYPTION SCHEME FOR FILE SHARING IN VIRTUAL CLOUD ENVIRONMENT

S. S. Aravinth[1], M. Ramkumar[2], A. Priyadharshini[3], E. Arun[4], G.Poovarasan[5], B. Mano Ranjitha[6]
[1,2,3]Asst Professor-CSE/ Knowledge Institute of Technology, Salem
[4,5,6]III - CSE/Knowledge Institute of Technology, Salem

Abstract- **Cloud computing users can share data files among dynamic groups in the cloud. A challenging issue at present is lag in guaranteeing the security for sharing the data file. The owner can upload the data files in the cloud by rend the services from the cloud service providers. According to the service level agreement the third party auditor will verify the uploaded files before accessing the data files from the cloud. The key distribution can be secured by providing a secure data sharing scheme for dynamic groups. The authorized application will generate the secret key to access the file. First the third party auditor will authorize the file request to be accessed by the user. Secondly, the authorized application will send the secret key to the user only when the uploaded files are verified. When a new user joins in the group or a user is revoked from the group. The previous users need not update their private keys. Finally the revoked users cannot get the original data file when they left the dynamics groups in the cloud.**

Index Terms- **Cloud computing, Revoked users, Authorized application., multi-authority**

I. INTRODUCTION

Cloud Computing:

Cloud computing is the way and model for delivering information technology services in which the computing resources are retrieved from internet rather than having local servers or personal devices.

II. LITERATURE SURVEY

Survey 1:
BAF: The Efficient Publicly Verifiable Secure Audit Logging Scheme for the Distributed Systems

Public key cryptography (PKC) based schemes for logging in task intensive or resource-constrained systems are more expensive. In the Symmetric schemes are not publicly verifiable. The forward secure and aggregate logging scheme called blind-aggregate-forward (BAF) logging scheme. BAF provides publicly verifiable forward secure and aggregate signatures with near-zero computational systems, storage systems and communication costs for the loggers, is a technique allows outsourcing of dynamic data to supports operations, without having any online trusted third party (TTP) support. BAF is secure, efficient and scalable. By using BAF a secure logging in both task intensive and resource-constrained systems is achieved.

Survey 2:
A Conclusive Data Possession at Untrusted Stores

The probabilistic proof's reduces I/O costs. The client maintains an amount of metadata to verify the proof. The protocol transmits a small, constant amount of data, minimizes network communication. The implementation of provable data possession reveals the performance of PDP is bounded by disk I/O and not by cryptographic computation.

Survey 3:
Innovative and Efficient Provable Data Possession

The storage server is assumed to be untrusted in terms of both security and reliability. By using the symmetric key cryptography technique bulk encryption can be reduced.

Survey 4:
Dynamic Provable Data Possession

In the provable data possession (PDP) model, the client's meta-data is preprocessed and sends to an untrusted server for storage. Without downloading the original data the client asks the server to prove that the stored data is not deleted. The PDP scheme is applied to the static files. A definitional framework and constructions for the dynamic provable data possession (DPDP) are provided to extend the PDP model to support provable updates to stored data. Authenticated dictionaries are implemented, which is based on rank information. File systems and version control systems are applied using DPDP scheme (e.g. CVS).

Survey 5:

An Efficient Provable Data Possession for Hybrid Clouds

In this paper, multiple cloud service providers store and maintain the client's data by having cooperative provable data possession which supports scalability of service and data migration in hybrid cloud.

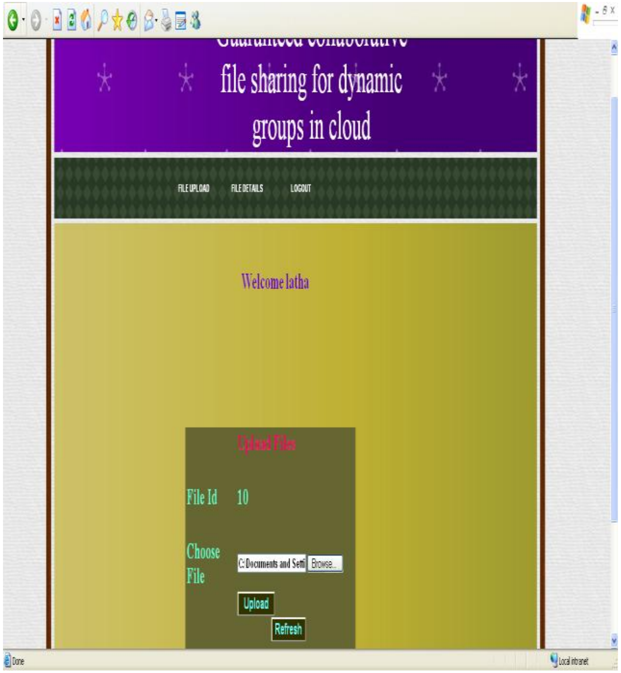
III. MODULES

- ❖ Tag Generation
- ❖ Key Generation
- ❖ Periodic Sampling Audit
- ❖ Audit for Dynamic Operations

IV. MODULES DESCRIPTION:

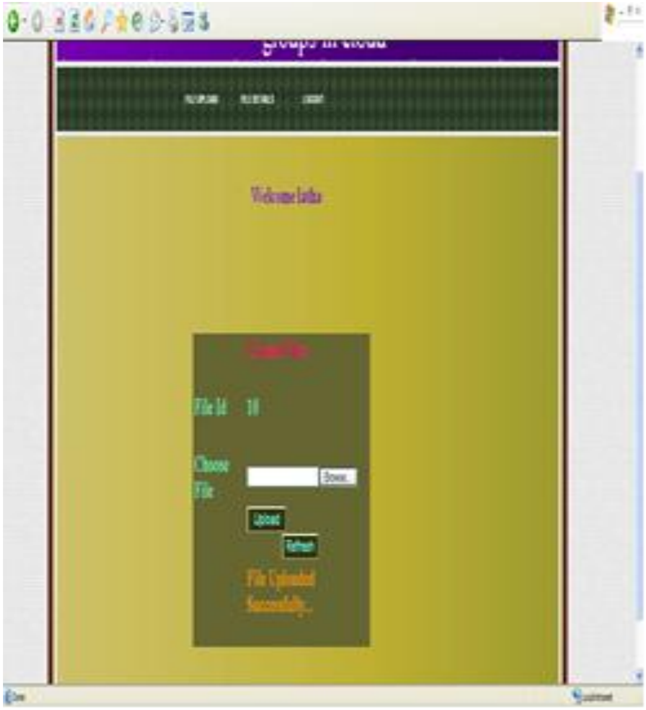
Tag Generation:

The client (data owner) uses the secret key sk to pre-process a file, which consists of a collection of n blocks, generates a set of public verification parameters and index-hash table that are stored in TPA, and transmits the file and some verification tags to CSP.



File Id 10

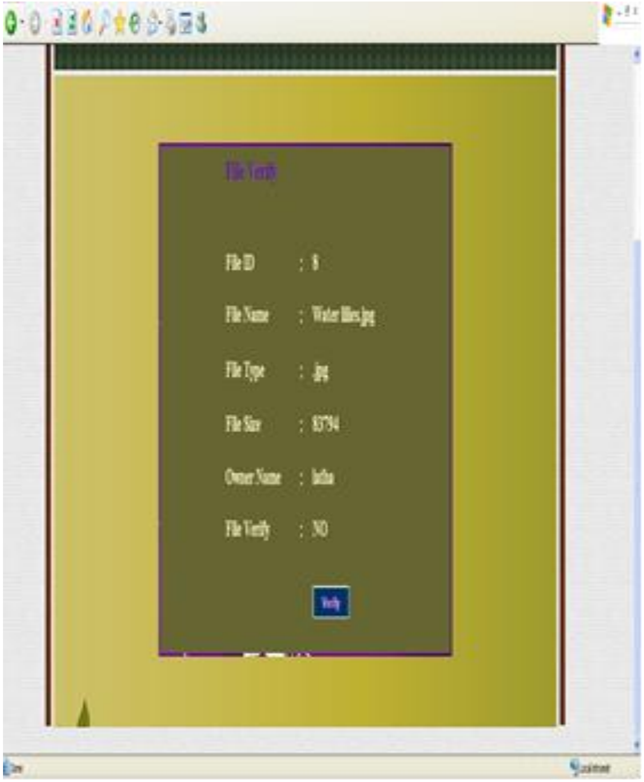
Choose File C:\Documents and Setti



File Id 10

Choose File

File Uploaded Successfully...



File ID : 8

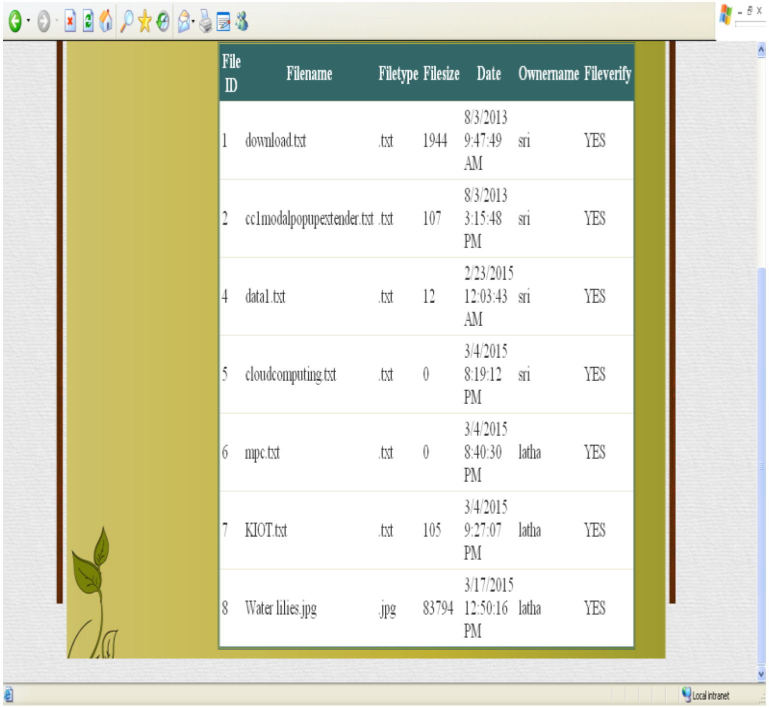
File Name : Water lilies.jpg

File Type : jpg

File Size : 83794

Owner Name : latha

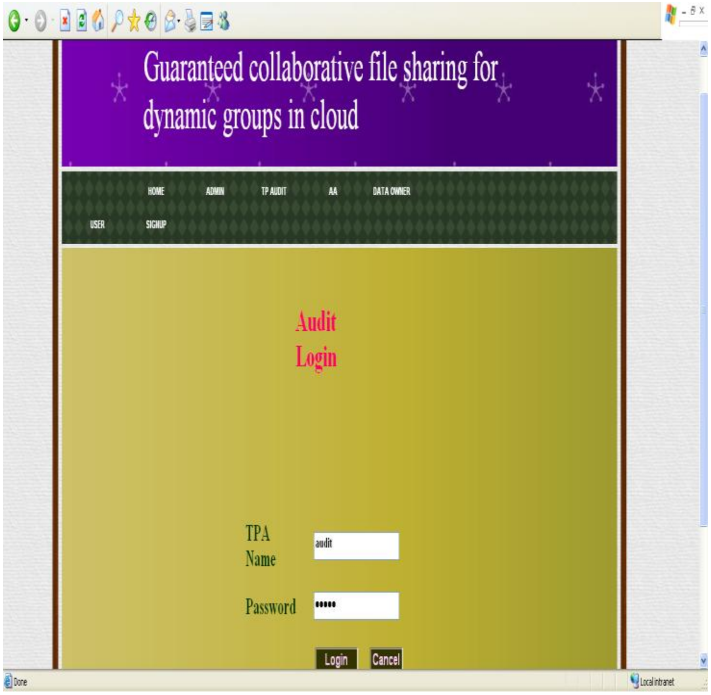
File Verify : NO



File ID	Filename	Filetype	Filesize	Date	Ownername	Fileverify
1	download.txt	.txt	1944	8/3/2013 9:47:49 AM	sri	YES
2	cc1modalpopupextender.txt	.txt	107	8/3/2013 3:15:48 PM	sri	YES
4	data1.txt	.txt	12	2/23/2015 12:03:43 AM	sri	YES
5	cloudcomputing.txt	.txt	0	3/4/2015 8:19:12 PM	sri	YES
6	mpc.txt	.txt	0	3/4/2015 8:40:30 PM	latha	YES
7	KIOT.txt	.txt	105	3/4/2015 9:27:07 PM	latha	YES
8	Water lilies.jpg	.jpg	83794	3/17/2015 12:50:16 PM	latha	YES

Key Generation:

The owner generates a public/secret key pair (pk, sk) by himself or else the system manager ,and finally then sends his public key pk to TPA. Note that TPA not obtain the client’s secret key sk.



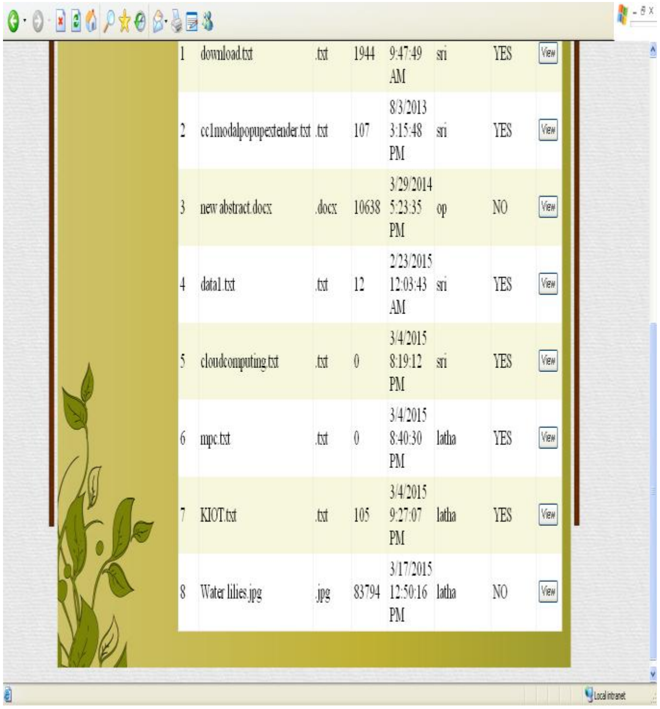
Guaranteed collaborative file sharing for dynamic groups in cloud

Audit Login

TPA Name: audit

Password: •••••

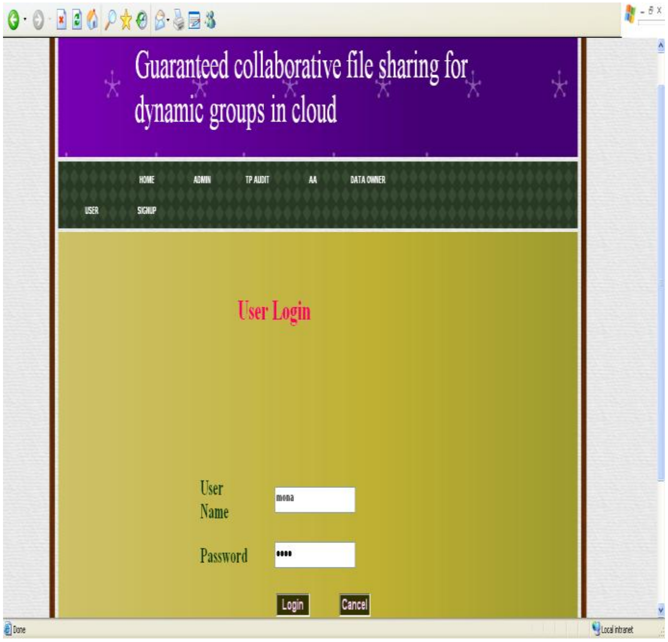
The owner may chooses the random secret.



1	download.txt	.txt	1944	9:47:49 AM	sri	YES	View
2	cc1modalpopupextender.txt	.txt	107	8/3/2013 3:15:48 PM	sri	YES	View
3	new abstract.docx	.docx	10638	3/29/2014 5:23:35 PM	op	NO	View
4	data1.txt	.txt	12	2/23/2015 12:03:43 AM	sri	YES	View
5	cloudcomputing.txt	.txt	0	3/4/2015 8:19:12 PM	sri	YES	View
6	mpc.txt	.txt	0	3/4/2015 8:40:30 PM	latha	YES	View
7	KIOT.txt	.txt	105	3/4/2015 9:27:07 PM	latha	YES	View
8	Water lilies.jpg	.jpg	83794	3/17/2015 12:50:16 PM	latha	NO	View

Periodic Sampling Audit:

TPA (or other applications) issues a “Random Sampling” challenge to audit the integrity and availability of outsourced data in terms of the verification information has been stored in TPA. In contrast with “whole” checking, random “sampling” checking greatly reduces the workload of audit services,also it has been achieves an effective detection of misbehaviors. a



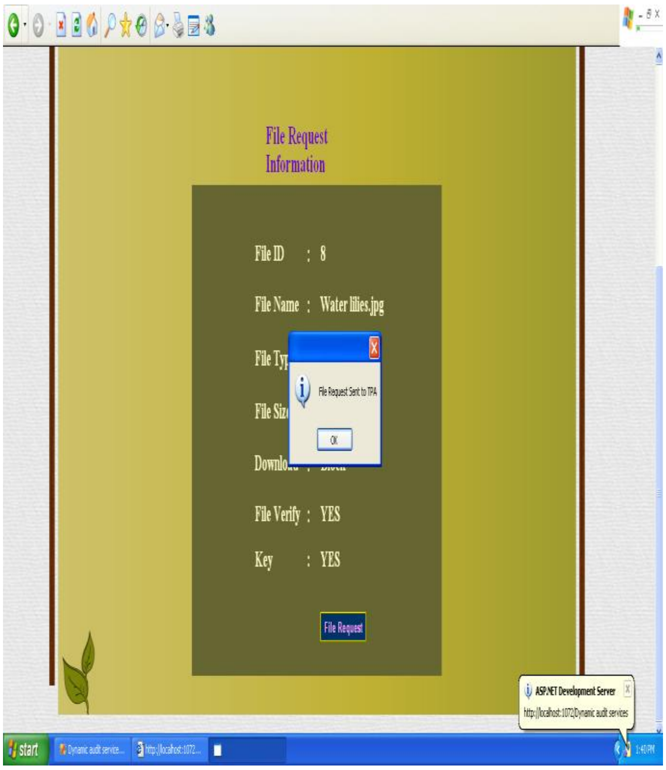
Guaranteed collaborative file sharing for dynamic groups in cloud

User Login

User Name: mona

Password: ••••

probabilistic audit on sampling checking is preferable to realize the anomaly detection in a timely manner, and as well as to rationally allocate resources.



File Request Information

File ID : 8

File Name : Water lilies.jpg

File Typ

File Siz

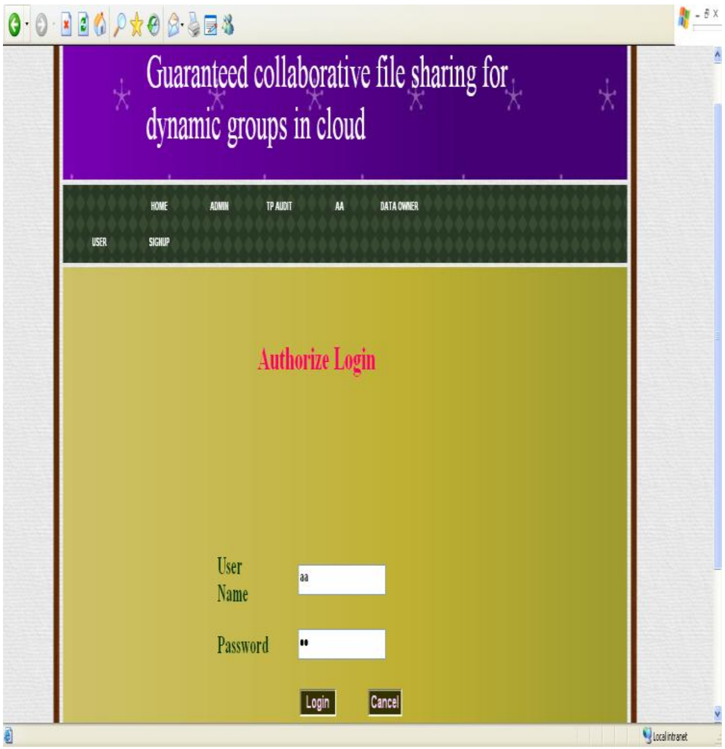
Downlo

File Verify : YES

Key : YES

File Request Sent to TPA

OK
File Request
ASP.NET Development Server
http://localhost:1072/Dynamic audit services
start
Dynamic audit service...
http://localhost:1072...

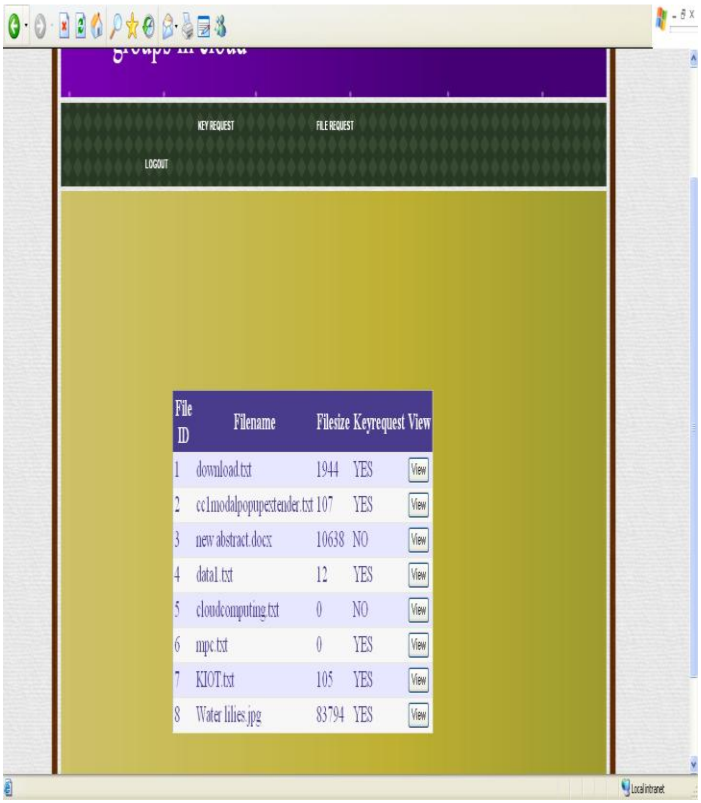


Guaranteed collaborative file sharing for dynamic groups in cloud

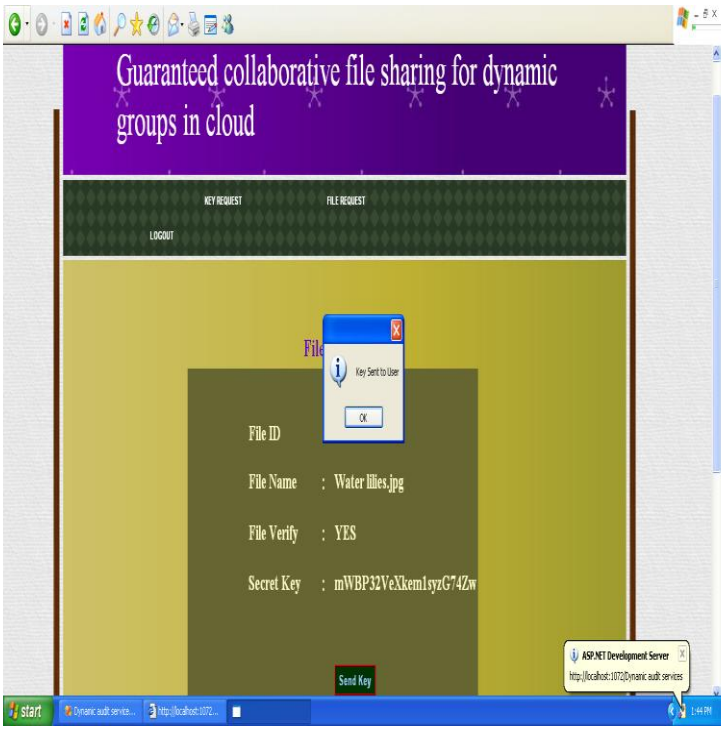
Authorize Login

User Name: aa

Password: ••



File ID	Filename	Filesize	Keyrequest	View
1	download.txt	1944	YES	View
2	cc1modalpopupextender.txt	107	YES	View
3	new abstract.docx	10638	NO	View
4	data1.txt	12	YES	View
5	cloudcomputing.txt	0	NO	View
6	mpc.txt	0	YES	View
7	KIOT.txt	105	YES	View
8	Water lilies.jpg	83794	YES	View



Guaranteed collaborative file sharing for dynamic groups in cloud

File

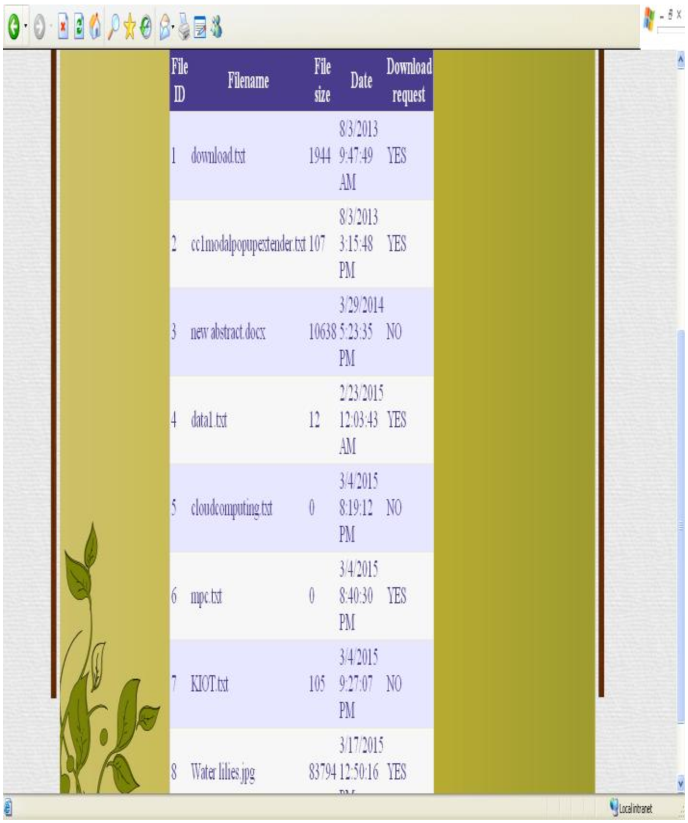
File ID

File Name : Water lilies.jpg

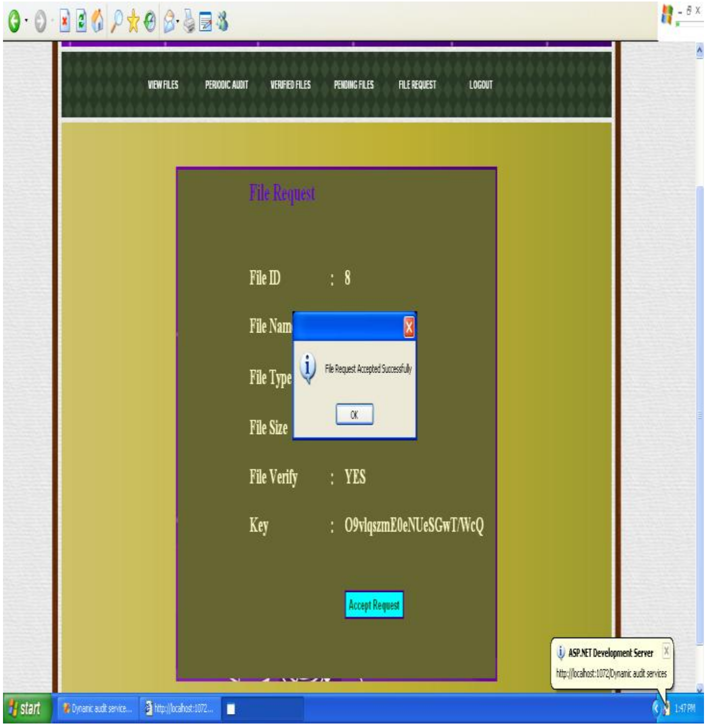
File Verify : YES

Secret Key : mWBP32VeXkem1syzG74Zw

Key Sent to User



File ID	Filename	File size	Date	Download request
1	download.txt	1944	8/3/2013 9:47:49 AM	YES
2	cc1modalpopupextender.txt	107	8/3/2013 3:15:48 PM	YES
3	new abstract.docx	10638	3/29/2014 5:23:35 PM	NO
4	data1.txt	12	2/23/2015 12:03:43 AM	YES
5	cloudcomputing.txt	0	3/4/2015 8:19:12 PM	NO
6	mpc.txt	0	3/4/2015 8:40:30 PM	YES
7	KIOT.txt	105	3/4/2015 9:27:07 PM	NO
8	Water lilies.jpg	83794	3/17/2015 12:50:16	YES



File Request

File ID : 8

File Nam

File Type

File Size

File Verify : YES

Key : O9vlqszmE0eNUeSGwT/WcQ

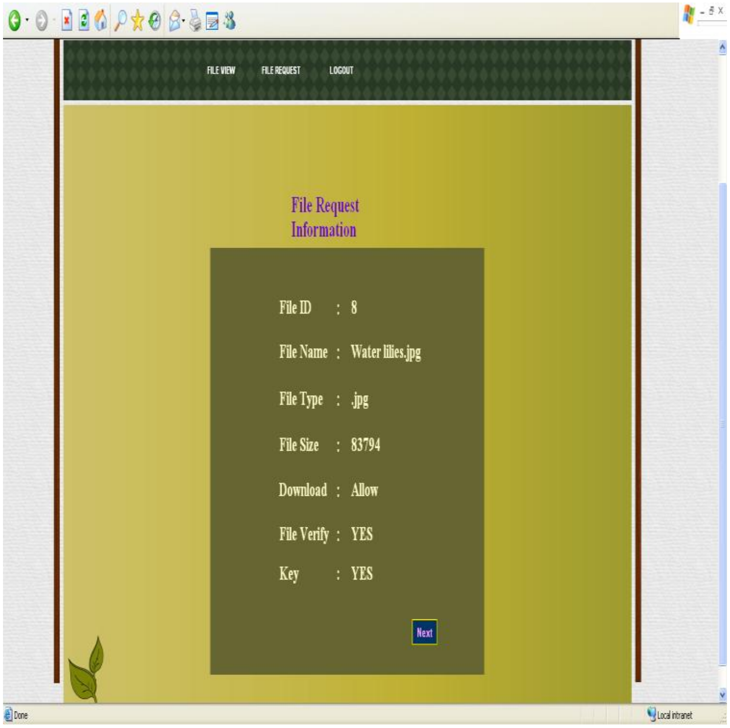
File Request Accepted Successfully

ASP.NET Development Server

http://localhost:1072/Dynamic audit services

Audit for Dynamic Operations:

An authorized application, that holds the knowledge owner's secret key (sk),that will manipulate the outsourced knowledge and update the associated index hash table will hold on in TPA. The privacy of sk may checking formula make sure that the storage server cannot cheat the licensed applications and forge the valid audit records.



File Request Information

File ID : 8

File Name : Water lilies.jpg

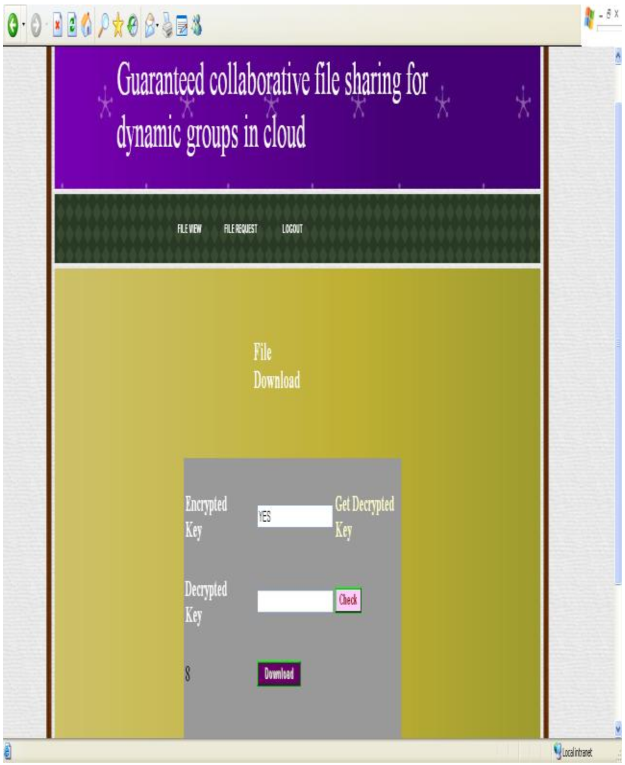
File Type : .jpg

File Size : 83794

Download : Allow

File Verify : YES

Key : YES



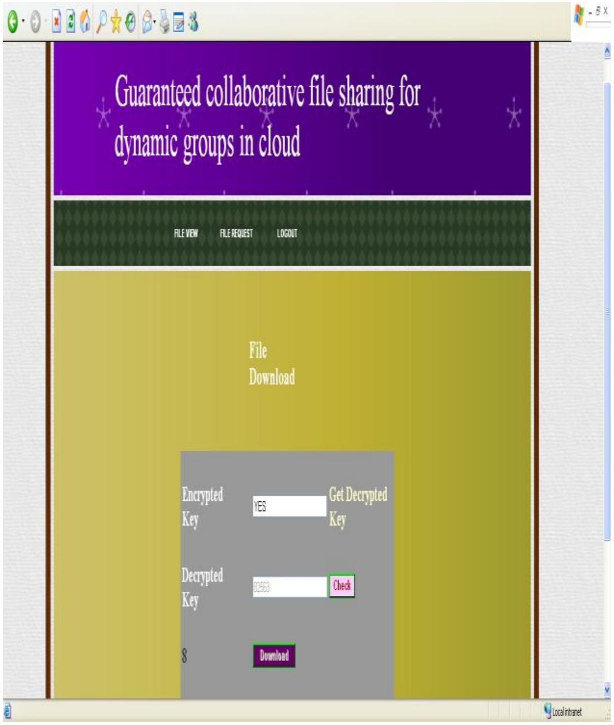
Guaranteed collaborative file sharing for dynamic groups in cloud

File Download

Encrypted Key: YES

Decrypted Key:

8



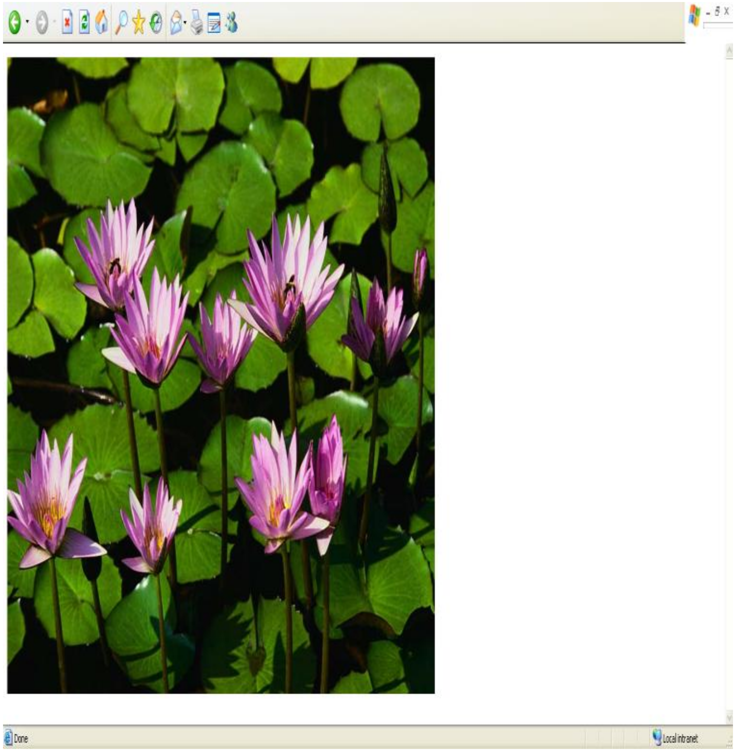
Guaranteed collaborative file sharing for dynamic groups in cloud

File Download

Encrypted Key: YES

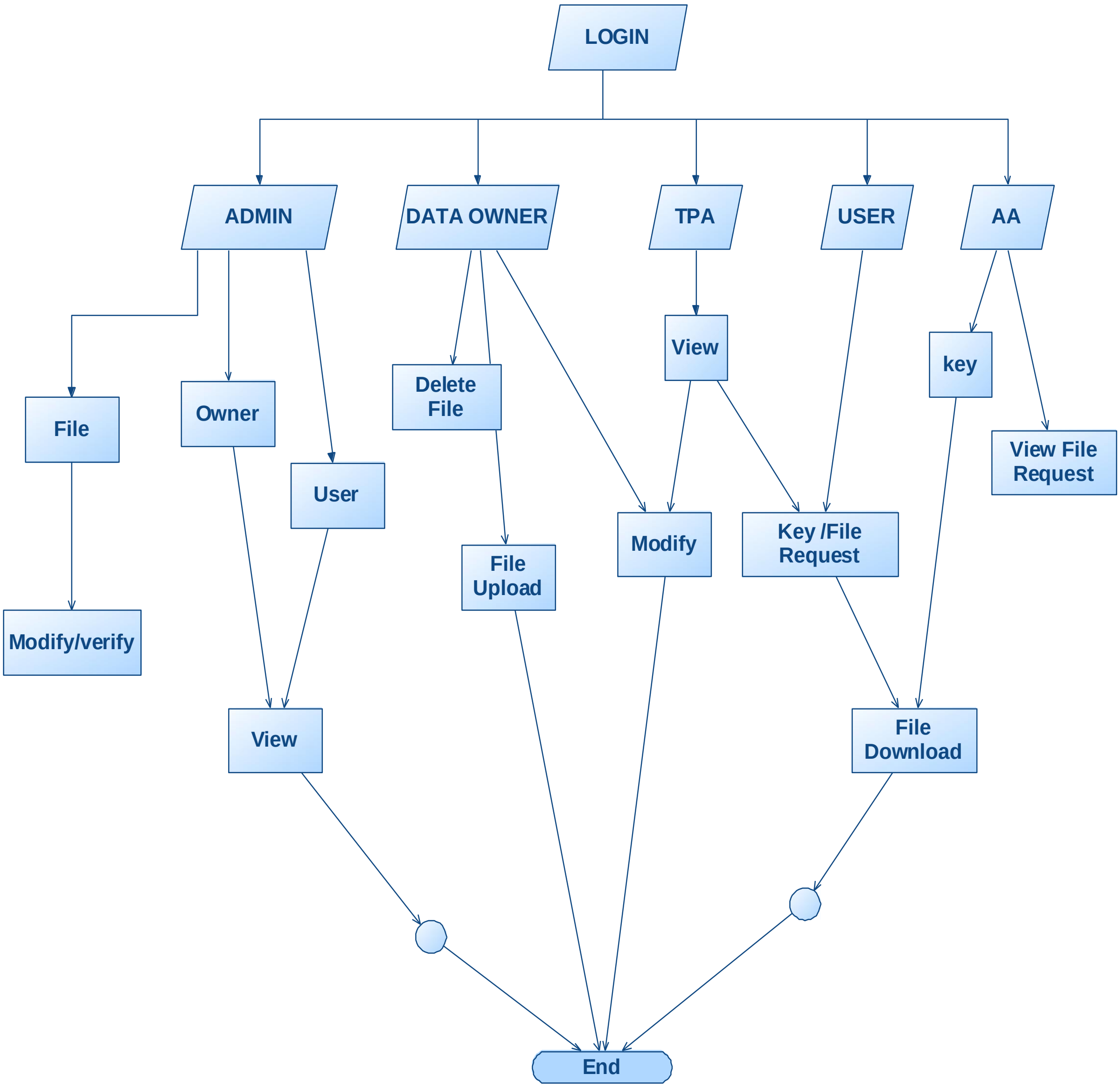
Decrypted Key: 82563

8



V. DATA FLOW DIAGRAM

- ✓ Enter into the login
- ✓ Data owner and User are registered and have their separate logins.
- ✓ The login page consists of Admin, Data owner, Third party auditor (TPA), User and Authorized application (AA).
- ✓ Data owner can upload the file and delete the file in the cloud.
- ✓ Admin verifies the uploaded file and allows the user to give file and key request.
- ✓ User can request the file and download the file.
- ✓ Third party auditor (TPA) sends the secret key to the user.
- ✓ Authorized application (AA) accepts the file request and allows the used to view and access the data file.



VI. CONCLUSION

The implementation of a data files to be shared among the dynamic groups in the cloud. The third party auditors allow only the valid users to access the data files among the dynamic groups. The original data files cannot be accessed by the revoked users. The previous users need not update their private keys either a new user joins in the group or a user is revoked from the group.

VII. FUTURE ENHANCEMENT

Future work will extend the application of alert message provided by the third party auditor which indicates the validity of services provided by the cloud service providers. So that, the clients will know the expiry of the services rented and update their services

REFERENCES

[1] Amazon Web Services, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.

[2] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007

[3] M. Mowbray, "The Fog over Grimpen Mire: Cloud Computing and the

Law," Technical Report HPL-2009-99, HP Lab., 2009.

[4] A.A. Yavuz and P. Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009.

[5] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007