Dynamic Groups based Data Sharing Scheme in the Cloud

Korra Santhosh Kumar Naik & Mrs. B.Deepthi Reddy
1.M.TechScholar,DepartmentofIT,J.B.InstituteofEngineering&Technology,Hyderabad,Telangana.
Email:santhosh81253@gmail.com.
2. Assistant Professor, Department of IT, J.B. Institute of Engineering & Technology, Hyderabad, Telangana.
Email:deepthi.bhonagiri@gmail.com

ABSTRACT

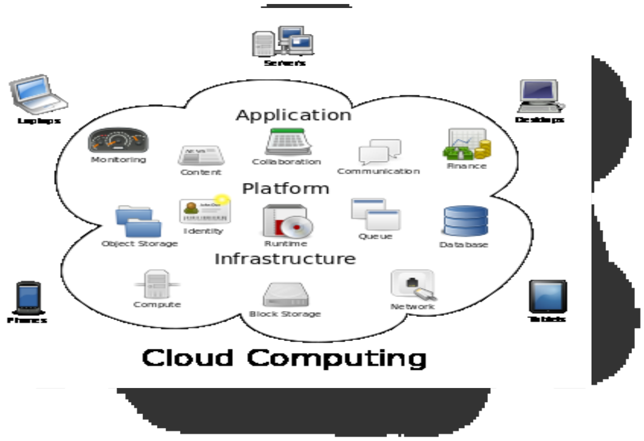
Profited from distributed computing, clients can accomplish a compelling and temperate approach for information sharing among assemble individuals in the cloud with the characters of low upkeep and little administration cost. In the mean time, we should give security certifications to the sharing information documents since they are outsourced. Sadly, on account of the continuous difference in the participation, sharing information while giving protection saving is as yet a testing issue, particularly for an untrusted cloud because of the agreement assault. In addition, for existing plans, the security of key dissemination depends on the safe correspondence channel, notwithstanding, to have such channel is a solid presumption and is troublesome for training. In this paper, we propose a protected information sharing plan for dynamic individuals. Right off the bat, we propose a safe path for key appropriation with no safe correspondence channels, and the clients can safely acquire their private keys from bunch director. Also, our plan can accomplish fine-grained get to control, any client in the gathering can utilize the source in the cloud and repudiated clients can't get to the cloud again after they are renounced. Thirdly, we can shield the plan from arrangement assault, which implies that disavowed clients can't get the first information document regardless of the possibility that they plot with the untrusted cloud. In our approach, by utilizing polynomial capacity, we can accomplish a safe client denial plot. At last, our plan can accomplish fine proficiency, which implies past clients require not to refresh their private keys for the circumstance either another client participates in the gathering or a client is denied from the gathering.

INTRODUCTION

Cloud computing

is the utilization of processing assets (equipment and programming) that are conveyed as an administration over a system (regularly the Internet). The name originates from the normal utilization of a cloud-molded image as a reflection for the unpredictable framework it contains in framework charts.

Distributed computing depends remote administrations with a client's information, programming and calculation. Distributed computing comprises of equipment and programming assets made accessible on the Internet as oversaw outsider administrations. These administrations commonly give access to cutting edge programming applications and top of the line systems of server PCs.



Purpose:

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud. Abstract: ... Second, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

Scope:

The scope of this paper tends to our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group

LITERATURE SURVEY

1 "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,"

AUTHORS: B. Wang, B. Li, and H. Li,

2 Security Challenges for the Public Cloud,"

AUTHORS: K. Ren, C. Wang, and Q. Wang,

3 Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"

AUTHORS: C. Wang, Q. Wang, K. Ren, and W. Lou

SYSTEM ANALYSIS

EXISTING SYSTEM:

Kallahalla et al demonstrated a cryptographic securing framework that draws in secure information sharing on boggling servers in light of the techniques that isolating archives into record get-togethers and encoding each record assemble with a report piece key.

Yu et al manhandled and joined philosophies for key approach trademark based encryption, center solitary re-encryption and idle re-encryption to satisfy fine-grained information find the opportunity to control without revealing information substance.

Proposed System :

We propose a guaranteed information sharing outline, which can accomplish secure key course and information sharing for dynamic gathering. We give an ensured approach to manage administer key headway with no secured.

An affiliation exists on a host, and is seen by its port. This is a 16 bit number. To set up a relationship on a server, you send it to the port for that relationship of the host that it is running on. This is not zone straightforwardness! Without question of these ports are "outstanding".

Feasibility Study:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- OPERATIONAL FEASIBILITY
- TECHNICAL FEASIBILITY

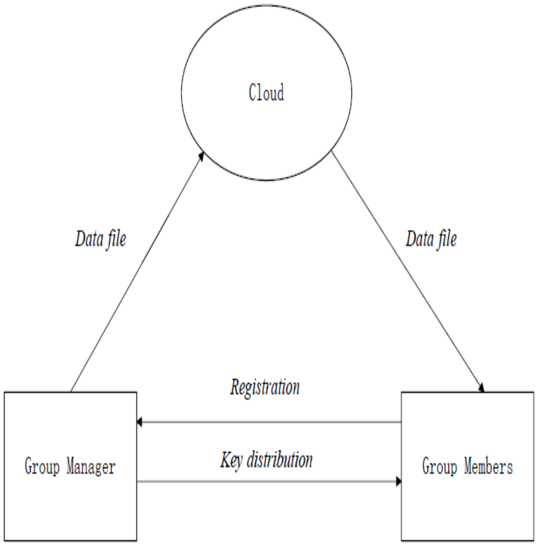
Hardware Requirements

System	:	Pentium IV 2.4 GHz.
Hard Disk	:	40 GB.
Monitor	:	15 VGA Colour.
Mouse	:	Logitech.
Ram	:	512 Mb.

Software Requirements

- Java Development Kit 1.8.
- Coding language – Java
- Project Coding - Eclipse Kepler IDE Tool
- Database - MySQL
- Server - Apache Tomcat.7
- Operating System-Windows XP, Windows -7

SYSTEM DESIGN System Architecture:



IMPLEMENTATION

Technology Used:

Technologies used in implementation are Anti Collusion technologies by using Polynomial Function.

MODULES:

1.Cloud Module

2.Group Manager Module

3.Group Member Module

4.File Security Module

5.Group Signature Module

6. User Revocation Module .

MODULES DESCRIPTION:

1.Cloud Module :

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

2.Group Manager Module :

Group manager takes charge of followings:

1. System parameters generation,

2. User registration,

3. User revocation, and

4. Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

3.Group Member Module :

Group members are a set of registered users that will

1. Store their private data into the cloud server and
2. Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

4.File Security Module :

1. Encrypting the data file.

2. File stored in the cloud can be deleted by either the group manager or the data owner.

(i.e., the member who uploaded the file into the server).

5.Group Signature Module :

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

6. User Revocation Module :

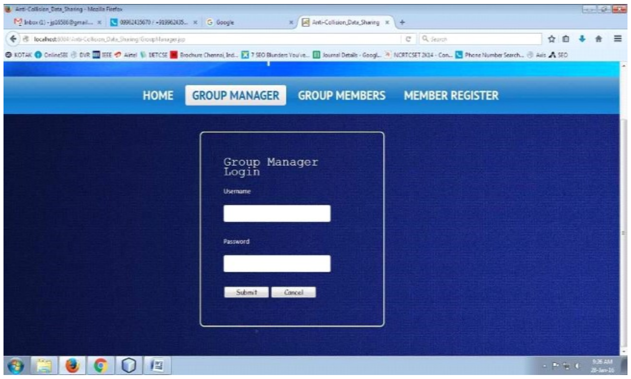
User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users

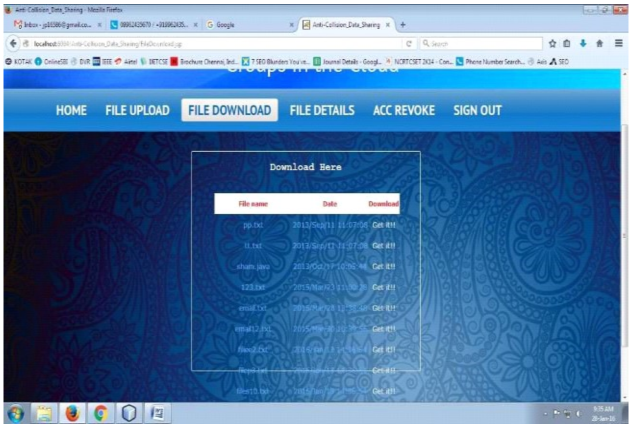
TESTING

Unit testing

Integration testing
Functional test
System Test
White Box Testing
Black Box Testing

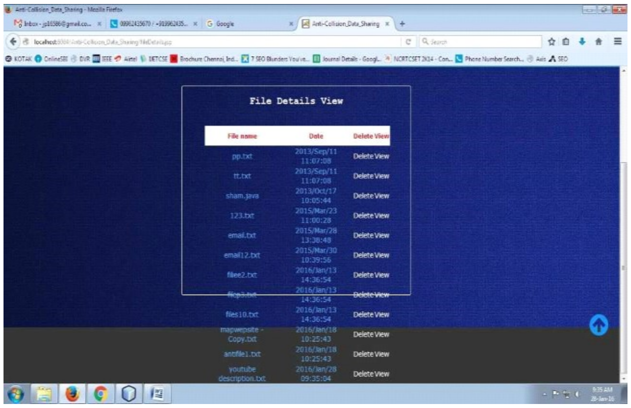
RESULT SCREENS





Download Here

File name	Date	Download
pp.txt	2013/Sep/11 11:07:08	Get it!!
tt.txt	2013/Sep/11 11:07:08	Get it!!
sham.java	2013/Oct/17 10:05:44	Get it!!
123.txt	2015/Mar/23 11:00:28	Get it!!
email.txt	2015/Mar/28 13:38:48	Get it!!
email12.txt	[illegible]	Get it!!
filee2.txt	[illegible]	Get it!!
[illegible]	[illegible]	Get it!!
files10.txt	[illegible]	Get it!!



File Details View

File name	Date	Delete View
pp.txt	2013/Sep/11 11:07:08	Delete View
tt.txt	2013/Sep/11 11:07:08	Delete View
sham.java	2013/Oct/17 10:05:44	Delete View
123.txt	2015/Mar/23 11:00:28	Delete View
email.txt	2015/Mar/28 13:38:48	Delete View
email12.txt	2015/Mar/30 10:39:56	Delete View
filee2.txt	2016/Jan/13 14:36:54	Delete View
[illegible]	2016/Jan/13 14:36:54	Delete View
files10.txt	2016/Jan/13 14:36:54	Delete View
mapwepsite - Copy.txt	2016/Jan/18 10:25:43	Delete View
antfile1.txt	2016/Jan/18 10:25:43	Delete View
youtube description.txt	2016/Jan/28 09:35:04	Delete View

CONCLUSION AND FUTURE SCOPE

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

References

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. "A View of Cloud Computing,"Comm. ACM, vol. 53,no.4, pp.50-58, Apr.2010.

[2] S.Kamara and K.Lauter,"Cryptographic Cloud Storage," Proc.Int'l Conf.Financial Cryptography and Data Security (FC), pp.136-149, Jan. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4] E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.