Secured Image Sharing and Deletion in the Cloud Storage Using Access Policies

Nishana Rahim
PG Student, Department of Computer Science & Engineering
Regional Centre of Anna University
Tirunelveli, India
nishanrahim@gmail.com

K. Saravanan
Assistant Professor, Department of Computer Science & Engineering
Regional Centre of Anna University
Tirunelveli, India
saravanan.krishnann@ gmail.com

***Abstract*— Cloud computing is a general term for anything that involves delivering hosted services, Anything as a Service (AaaS), over the web on demand basis. It uses web and central remote servers to maintain data and applications. Outsourcing data storage and maintenance to third-party cloud services reduces data management costs, but providing security guarantees is a major issue. In this approach, a secured cloud storage system that achieves policy-based access control and file assured deletion is proposed with an information accountability cloud framework to keep track of the actual usage of the clients' data. Automated logging and distributed auditing of relevant access performed by any entity is handled. The access policy generated for the file controls the file accesses and policy revocation makes the file permanently inaccessible. The system is built upon a set of cryptographic key operations that are self-maintained by a set of key managers and adds security features.**

Keywords- Policy; access control; assured deletion; logging; auditing

I. INTRODUCTION

Cloud storage enables clients to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. A cloud service has three distinct characteristics that differentiate it from traditional hosting: 1) It is sold on demand, 2) It is elastic, so a client can have as much or as little of a service as they want at any given time 3) The service is fully managed by the provider.

Cloud computing allows consumers and businesses to use applications without installation & maintenance and access their personal files at any computer with web access. Cloud computing provides efficient storage and computing services. It is inexpensive, since all the virtual resources (applications or hardware or data) are covered by the service provider. It allows for easy connectivity to servers and information sharing. It assures appropriate use of resources as the clients are required to pay only for the services they require. It is highly reliable and redundant. This sets the business people free from the hassles of buying, managing and maintaining all the virtual resources at their own end, the cloud server does it all.

A cloud system may have many cloud service providers (CSPs) to improve the performance. Based on availability and work load, the system selects a CSP for the client accessing it. Hundreds or thousands of clients may access the system simultaneously; hence the availability is a major problem. It can be improved by CSPs with data replication. Since the data and data owner is same for all copies of the data, this causes another concern of accountability. So the owner has to aware about the copies of data and who all are using it. Since the data is storing remotely; the data owner is unaware of where the data is located and how many copies are created. This may lead to unauthorized access of the data. The data owner may want to set some restrictions to clients who are trying to access the data. In this scenario, the distributed data should keep all these details. But again the authorized clients should be categorized according to permission; it will be a problem in a distributed system with many clients.

A cloud framework is created for secured data sharing. This performs automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider. Cloud Framework has two major components: logger and log harmonizer. The logger is the component which is strongly coupled with the owner's data, so that it records each and every access to the data by any other client. The log harmonizer forms the central component which allows the data owner to access the log files. The security is again a major concern. To overcome these problems, a new approach is proposed for secured data sharing with authentication.

The system allows clients to be timely and accurately informed about their data usage. The proposed system allows image sharing in a secured manner. The data owner can share images with access permissions. Each

image/file has some access control and only authorized clients can access the images/files. Assured deletion of files, which promise permanent deletion from the storage, is another feature. To provide guarantees of access control and assured deletion, cryptographic schemes including threshold secret sharing and attribute based encryption (ABE) are using. This paper presents secured cloud storage for image sharing with access policies. The clients of the system must satisfy certain access policies to access the images/files stored. The files are stored along with file access policies and for assured deletion the corresponding policies are revoked and hence the files are permanently inaccessible for clients. The access information is recorded and the owners can check it.

In this paper, section 2 discusses the related works and some techniques used for security. The section 3 explains system overview and different components of the system architecture. Section 4 deals with security features and section 5 says about the implementation of the cloud framework with automated logging and auditing. Section 6 discusses the performance evaluation and section 7 concludes the work so far.

II. RELATED WORK

According to the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4]. A characteristic of cloud computing is its ability to be accessed anywhere there is a reliable web connection and hence availability is promoted in the cloud model. Cloud computing has raised a range of important privacy and security issues. Such issues are due to the fact that, users' data and applications reside, at least for a certain amount of time, on the cloud cluster which is owned and maintained by a third party.

Here the principal goal is to identify privacy and confidentiality issue that are primary interest and concern to cloud computing participants and users. Current privacy regulations are clearly not enough to solve all the privacy issues related to cloud computing. AlSudiari and Vasista [2] discussed the possible issues and regulations in the area of privacy that affect the implementation of cloud computing technologies. This helps to understand the issues to be faced in the cloud storage services. Similarly, article [5] also explained the cloud computing technology architecture and the cloud computing data security features. A cloud computing data security model can be raised with user authentication. Users who pass the authentication can get relative operation on the user data, such as addition, modification or deletion.

A detailed analysis of the cloud computing security issues and challenges is discussed in [6], which is focusing on the cloud computing types and the service delivery types and helps to understand the behavior of clients/users. That mainly proposes the core concept of secured cloud computing which suggests the cloud computing based on separate encryption and decryption services. Even though it suggests methods to avoid threats, solutions for the same are not specified.

The proposed architecture uses some important security services including authentication, encryption and decryption. The same is discussed along with compression in [7]. Key Policy Attribute-Based Encryption (KP-ABE), Proxy Re-Encryption (PRE) and Lazy re-encryption [7] handles many of the security issues. A main issue in the proposed system is distributed auditing. A flexible distributed storage integrity auditing mechanism, utilizing the 'homomorphic' token and distributed erasure-coded data is referred in [10]. The design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization. Considering the cloud data are dynamic in nature, the design [10] further supports secure and efficient dynamic operations on outsourced data, including block modification and deletion

Users' fears of losing control of their own data can become a significant barrier to the wide adoption of cloud services. This problem is addressed in [1] and they propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. Identity Based Encryption [8] Techniques are used for authentication and data security. In particular, an object-centred approach that enables enclosing our logging mechanism together with users' data and policies also proposed. The common attacks are copying attack, disassembling attack, man-in-the-middle attack and compromised JVM attack [1]. The main issues are overhead added by JVM integrity checking, authentication delay and storage overhead due to large log files. Another technique suggested for secured storage and authentication so far is Attribute Based Encryption [9]. The client based authentication requires access to key and policy of every client, which limits the scalability and flexibility. Attribute based encryption is the appropriate solution for scalability issue.

III. SYSTEM OVERVIEW

The clients are requested to register before sharing and accessing their images. The data owners upload their images with certain access policies. The images are encrypted for secured storage and kept in the cloud along with necessary keys. The keys are shared among a set of key managers. On the other hand, clients other than data owners request for images. The clients must satisfy certain access policies to access an image. The log records generated automatically during the access, which is also kept in encrypted format.

A. *Access Policy Generation*

Policies are created for access control. The clients have to register before accessing the system. An access control policy, for example, client-A can read and download files, is created for each client along with an access key. Similarly, each file also has a file access policy and unique control key. For example, file B can be viewed by clients from India only. The policies are stored in the cloud storage along with corresponding identity attribute. The client can access the file only if the access policy satisfies with file access policy.

B. *File Upload*

Each file has a file policy and associated control key. For each policy i, the key manager generates two secret large RSA prime numbers p_i and q_i and computes the product $n_i = p_i q_i$. The key manager then randomly chooses the RSA public-private control key pair (e_i, d_i). The parameters (n_i, e_i) will be publicized, while d_i is securely stored in the key manager. For uploading, the client first requests the public control key (n_i, e_i) of policy P_i from the key manager. Then the client generates two random keys K and S_i, and sends $\{K\}_{Si}$, S_i^{ei} and $\{F\}_K$ to the cloud. Then the client must discard K and S_i.

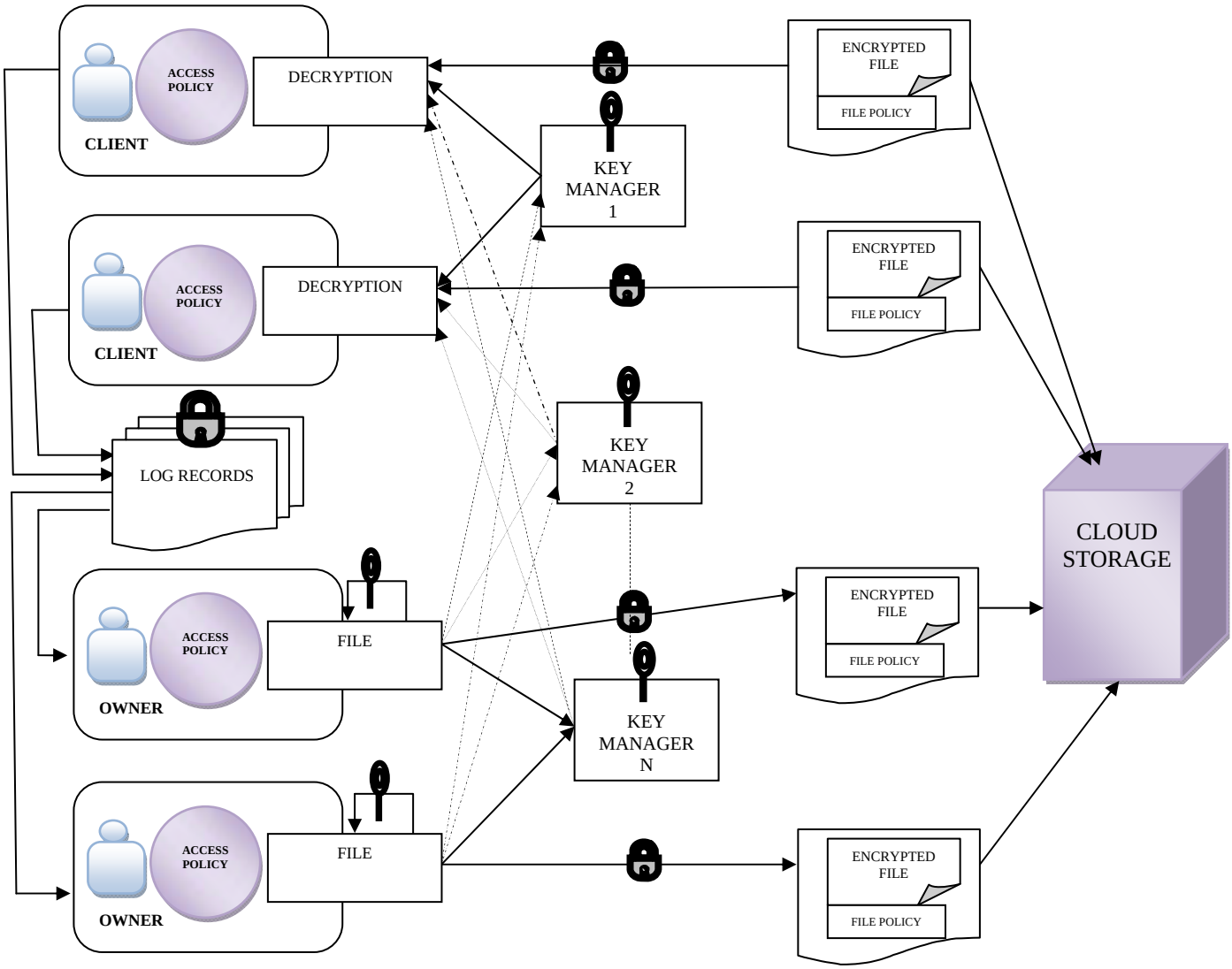

Figure 1. The System Overview

C. *File Download*

The design is based on blinded RSA, in which the client requests the key manager to decrypt a blinded version of the encrypted data key. If the associated policy is satisfied, then the key manager will decrypt and return the blinded version of the original data key. The client can then recover the data key. The motivation of using this blinded decryption approach is, the actual content of the data key remains confidential to the key manager as well as to any attacker that sniffs the communication between the client and the key manager.

The client fetches $\{K\}S_i$, S_i^{ei}, and $\{F\}K$ from the cloud. Then the client generates a secret random number R, computes R^{ei}, and sends S_i^{ei}. $R^{ei} = (S_iR)^{ei}$ to the key manager to request for decryption. The key manager then computes and returns $((S_iR)^{ei})^{di} = S_iR$ to the client, which can now remove R and obtain S_i, and decrypt $\{K\}S_i$ and hence $\{F\}K$.

D. File Deletion

A file will be deleted (or permanently inaccessible) if its associated policies are revoked and become obsolete. That is, even if a file copy that is associated with revoked policies exists, it remains encrypted and we cannot retrieve the corresponding cryptographic keys to recover the file. Thus the file copy becomes unrecoverable by anyone (including the owner of the file). If a policy P_i is revoked, then the key manager completely removes the private control key d_i and the secret prime numbers p_i and q_i. Thus, we cannot recover S_i from S_i^{ei}, and hence cannot recover K and file F. We say that file F, which is tied to policy P_i, is assuredly deleted. Note that the policy revocation operations do not involve interactions with the cloud.

E. Log Records

Log record is created for each access to images/files. The log record contains the id of the client/client accessed, image/file id, access policy of the client/client, access type, date, time and owner of the image. The logging mechanism is automated and distributed. The client can access images from any of the service providers. Each time the log record is stored in the log file. When a client trying to access an image, it is provided only after checking the permissions granted. Log file is encrypted using a random key and stored in the cloud. The key is again encrypted using access key of the owner. The access key is generated using the access permissions and identity attributes of the owner. The owner receives log files periodically and he/she can find out unauthorized accesses easily.

IV. SECURITY FEATURES

The system proposes a policy based file/image sharing and policy revocation for file assured deletion. The key managers are responsible for cryptographic key management. The main feature is that a file is encrypted using a data key by the owner of the file, and this data key is further encrypted by a control key by a separate key manager. Without the control key, the data key and hence the data file remain encrypted and are deemed to be inaccessible.

A. Cryptographic Keys

1) *Data Key*: The data key is a random secret key used to encrypt/decrypt files/log records using symmetric key encryption.
2) *Control Key*: The control key is associated with a particular file policy. It is a public-private key pair and the private control key is managed by a quorum of key managers. It is used to encrypt/decrypt data keys associated with files.
3) *Access Key*: The access key is associated with access policy of a client/owner. It is used to encrypt/decrypt data keys associated with log files.

B. Secret Key Sharing

In key sharing first create N key shares for a key, such that any $M \leq N$ of the key shares can be used to recover the key. To access files associated with active file policies, at least M out of N key managers required to keep the key shares of the required control keys. Then, to assuredly delete files, at least N - M + 1 out of N key managers must securely erase the corresponding control keys of the revoked policies. The parameters M and N determine the tradeoffs between the fault tolerance assumptions of key managers when accessing and deleting files. If M is small (large), then we need fewer (more) key managers to be active in order to access a file, but we need more (fewer) key managers to purge the revoked control keys in order to delete a file.

V. IMPLEMENTATION

The system is divided into many components to provide efficient storage and computing. The two scenarios, the admin and the client are separated in a gentle way and connected to appropriate functions. Cloud Framework is created based on the notion of information accountability. This framework performs automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider. It provides service for sharing the images of the admin and client. Simply the owner (client) shares data with certain access permissions provided by the system. The clients' with those permissions granted by the system can access the images. The log information is stored and can be viewed by owner.

The entire system is controlled by admin. Admin act as data owner also. The main functions of admin are checking the service request of the client and approving or rejecting the service. Only after confirmation, clients are permitted to log in to the system. The services are limited to the permission granted. Six kinds of permissions are allowed. They are 1) Read Only 2) Read and Download 3) Limited Time Read 4) Limited Time Download 5) Location Read 6) Location Download. Admin as well as clients share images by uploading new images and setting access permissions to the images which are the same as mentioned above. The images can be

deleted by the owner only. Log records are generated for each access. The client id and access policy is tracked for the log generation. Later this can be checked the owner.

Policy generation and policy revocation are two main functions. Each client of the system has an access policy and each file is uploaded with some file access policy. The policy is revoked for making the file inaccessible, which is termed as file assured deletion. A unique access key is generated for each client to protect identity information and log information. For secured image/file sharing, a unique random data key and associated control key is generated. A set of key managers keep the secret keys and provides whenever necessary.

Figure 2: User Service Approval by Admin

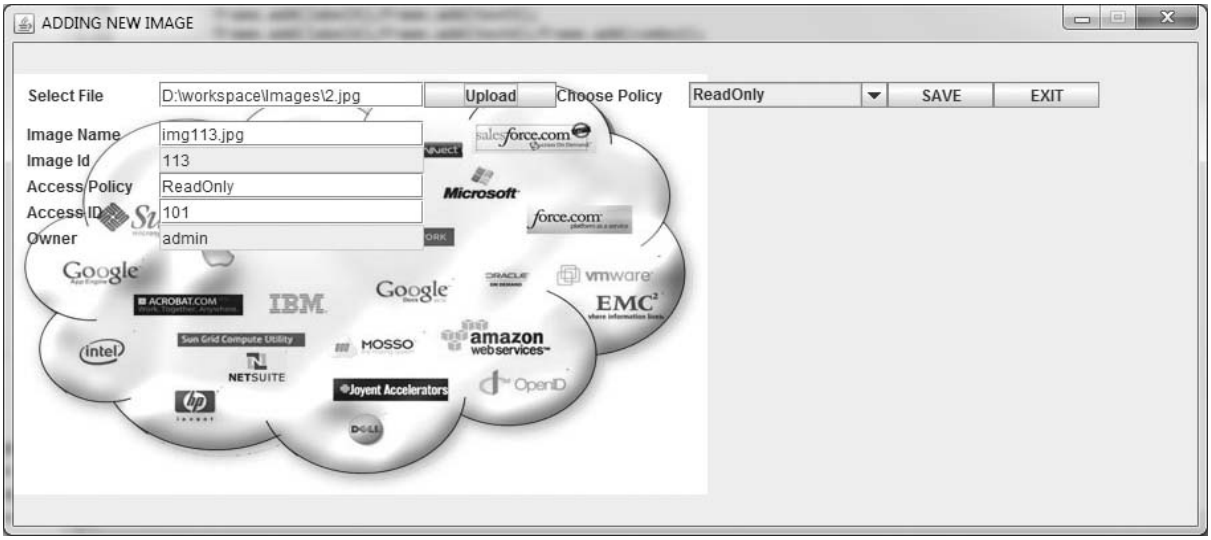

Figure 3: Uploading Image

VI. PERFORMANCE EVALUATION

Performance of the system should be evaluated with all the constraints and requirements. As the system provides cloud computing service, the system should satisfy the advantages of that. The throughput and security should reach some reasonable level. The main functions are logging and auditing. The processing of service request needs the attention of admin. The requests can be handled using admin for each service provider to improve the performance speed. Some performance constraints are listed below,

1) *Service Confirmation Time:* The time taken to grant a service request. If many users try to send request at same time or many users are waiting for confirmation, it will be a bottleneck for the CSP.

2) *Log Creation Time:* Finding out the time taken to create a log file when there are entities continuously accessing the data, causing continuous logging is a constraint.

3) *Authentication Time:* The overhead can occur is during the authentication of a CSP. If the time taken for this authentication is too long, it may become a bottleneck for accessing the enclosed data.

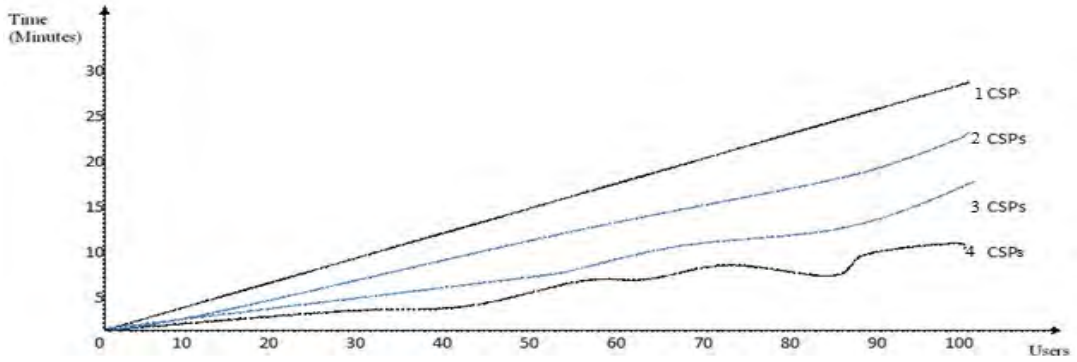

Figure 4: Service Confirmation [Users Vs Time] graph

A. Service Time

When many users send service request, with one service provider and admin, it is difficult to check and confirm all the requests without delay. The user has to wait for a reasonable time for getting account confirmation. It is the same, when many clients try to access the image files simultaneously. To avoid such delay more CSPs can be used. The graph, figure 4 illustrates this.

B. Cryptographic Operation Time

The total time for cryptographic operations includes the total computational time used for performing AES and RSA on the file and data key, and the time for the client to coordinate with the quorum of key managers on operating the cryptographic keys. For a client, the access to the system needs password decryption, data key decryption and file decryption. Similarly, an owner has to go through password decryption, control key generation, data key generation, file encryption and data key encryption. Hence both client and owner take a reasonable time for their operations.

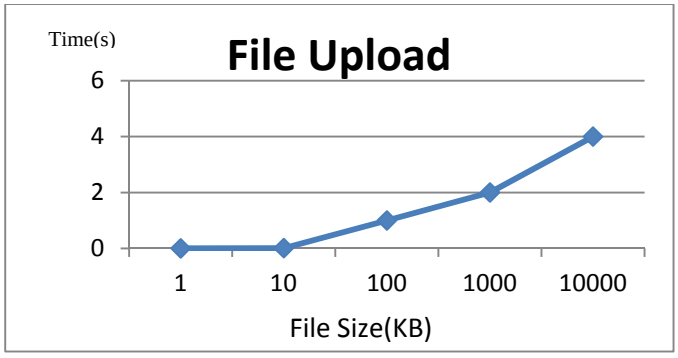

Figure 5: File Uploading [File size Vs Time] graph

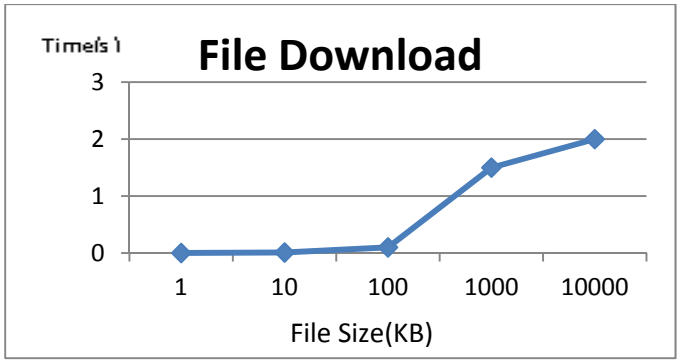

Figure 5: File Downloading [File size Vs Time] graph

C. Security

This system prevents the following two types of attacks. First, an attacker may try to evade the auditing mechanism by storing the files remotely, corrupting the file, or trying to prevent them from communicating with the owner. Second, the attacker may try to compromise the JRE used to run the files.

VII. CONCLUSION

The system proposed here provides a secured cloud storage system, which provides policy based file access and deletion. The policy will be generated for each client and file. The client, who satisfies the policies of the file, can access the file. A logging mechanism records the access information and auditing mechanism provides this information to the owner. The files and log records are kept as encrypted in the cloud storage system for avoiding various attacks. File assured deletion can be done by policy revocation, which removes the control key of the file from the database and hence the decryption of file is impossible. The functions of various cryptographic keys and operations are discussed along with key sharing. The performance evaluation reveals the constraints. The proposed system will be useful in image sharing when third party cloud storage is used.

REFERENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable And Secure Computing, Vol. 9, No. 4, July/August 2012

[2] Dr. Mohammed A. T. AlSudiari and Dr. TGK Vasista, "Cloud Computing and Privacy Regulations: An Exploratory Study on Issues and Implications," Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, March 2012

[3] Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem, "A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing," IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 3 (May-June 2012), PP 01-08

[4] Mell P. and Grance T. "NIST Definition of Cloud Computing V15." http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, May 2009.

[5] Zhang Xin , Lai Song-qing and Liu Nai-wen, "Research on cloud computing data security model based on multi-dimension," Information Technology in Medicine and Education (ITME), 2012 International Symposium, VOL. 2, **Page(s):** 897 – 900

[6] Kulkarni G; Dept. of Electron. & Telecommun., Marathwada Mitra Mandal's Polytech., Pune, India, Gambhir J, Patil T and Dongare A, "A security aspects in cloud computing," Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference

[7] S Sajithabanu and Dr. E George Prakash Raj, Dept. of Computer Science, Bharathidasan University, Trichy, Tamilnadu, India, "Data Storage Security in Cloud ," IJCST Vol. 2, Issue 4, Oct . - Dec. 2011

[8] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, May 2006

[10] Cong Wang, Dept. of Electr. & Comput. Eng., Illinois Inst. of Technol., Chicago, IL, USA , Qian Wang, Kui Ren, Ning Cao and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, VOL 5, Issue 2, April-June 2012

[11] Aderemi A. Atayero and Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption," Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, October 2011 ISSN 2079-8407

[12] Anthony Bisong and Syed (Shawon) M. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Computing," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

[13] Siani Pearson, Yun Shen and Miranda Mowbray, "A Privacy Manager for Cloud Computing," HP Labs, Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK, pp. 90-106, 2009

[14] Siani Pearson and Andrew Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," HP Laboratories, HPL-2009-178

[15] R. Corin, S. Etalle, J. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[16] Rodrigo N. Calheiros, Rajiv Ranjan, César A. F. De Rose and Rajkumar Buyya, CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services

[17] A. Boldyreva, V. Goyal and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), 2008.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS), 2006.

[19] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[20] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.14th Int'l Conf. Financial Cryptography and Data Security, 2010.

[21] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," Proc. 13th ACM Conf. Computer and Comm. Security (CCS), 2006.

[22] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), Apr. 2010.

AUTHORS PROFILE

Ms. Nishana Rahim, is an ME Computer Science & Engineering student at Regional Centre of Anna University, Tirunelveli. She recieved B.Tech Degree in Computer Science and Engineering from Cochin University of Science and Technology, Kerala.

Mr. K Saravanan, is working as an Assistant Professor, Department of Computer Science & Engg at Regional Centre of Anna University, Tirunelveli. He received his master degree in ME- Software Engineering in 2007 and BE degree in Computer Science. His research interest includes Grid and Cloud computing, Semantic Resource Allocation, Requirements Engineering and Software Metrics. He has published papers in several International & National conferences and 5 International Journals.