ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Anonymous Access Control and User Revocation with Log Managment in Cloud

Battuka Radha, B. Sasidhar

M.Tech Student, Dept. of Computer Science and Engineering, Mahaveer Institute of Science and Technology, Hyderabad, India.

Professor, Dept. of Computer Science and Engineering, Mahaveer Institute of Science and Technology, Hyderabad, India.

ABSTRACT: Access control is essential when unauthorized users try to access the data from the storage, so that only authorized users can access the data. It is also significant to verify that the information comes from a reliable source. We need to solve the problems of access control, authentication, and privacy protection by applying suitable encryption techniques. There are three types of access control: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data. This is not possible in clouds where there are many users. In RBAC users are classified based on their own roles. Data should be accessed by users who have matching roles. The roles are declared by the system. For an example, only faculty members and senior secretaries might have access to data but not the junior secretaries. In ABAC the user accessed by using user's credentials as attributes. In this paper we use ABAC and provides log management and revocation process.

KEYWORDS: Anonymity, attribute-based encryption, Log maintenance, user revocation.

I.INTRODUCTION

Cloud computing is that following generation in computation. Maybe Clouds can save the world; altogether likelihood people can have everything they need on the cloud. Cloud computing is that following natural step at intervals the evolution of on-demand data technology services and merchandise.

The Cloud could even be an image for Infobahn, supported but it's pictured in network diagrams, associated is Associate in nursing abstraction for the advanced infrastructure it conceals. it is a technique of computing throughout that IT-related capabilities unit provided "as a service", allowing users to access technology-enabled services from Infobahn (i.e., the Cloud) whereas not data of, expertise with, or management over the technology infrastructure that supports them. Email was presumptively the primary service on the "cloud". as a results of the computing business shifts toward providing Platform as a Service (PaaS) and code as a Service (SaaS) for shoppers and enterprises to access on demand in spite of it slow and portable computer, there will be an increase at intervals the vary of Cloud platforms offered. Cloud computing could even be very specific fairly computing that has terribly specific edges. But its specific negatives equally. Virtualization could even be a framework or methodology of dividing the resources of a transferable digital computer into multiple execution environments, by applying one or many ideas or technologies like hardware and code partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many of others. It permits abstraction and isolation of lower-level functionalities and underlying hardware. This permits quality of higher-level functions and sharing and/or aggregation of the physical resources. By this the tip user can access what unit of activity the resources needed for him.

Cloud computing could even be a paradigm that focuses on sharing data academic degreed computations over associate degree ascendible network of nodes. Samples of such nodes embrace user computers, data centers, and web Services. We've a bent to tend to tend to tend to term such a network of nodes as a cloud. Associate application supported such clouds is taken as a cloud application. Primarily cloud could even be an image for web associated is Associate in nursing abstraction for the advanced infrastructure it conceals. the foremost discovered is to use this infrastructure presently bring all potential services to the cloud and build it realizable to access those services in spite of it slow and portable computer. whether or not or not or not or not or not or not it's declared as Cloud Computing or On-demand computing, code as a Service or Infobahn as Platform, the common 0.5 could even be a shift at intervals the planet science of computation. Once you manufacture a program with the Google Docs service, major components of the code reside on unseen computers, whereabouts unknown, altogether chance scattered across continents. The benefits of the cloud computing unit of activity as follows

Reduced Cost: Cloud technology is paid incrementally (you pay only for what you need), saving organizations money at intervals the short run. Money saved unit of activity sometimes used for numerous necessary resources. Increased Storage: Organizations can store legion data than on personal portable computer notebook computer systems.

Highly Automated: IT personnel not needed to remain code up to this purpose as maintenance is that the duty of the service provider on the cloud. More Mobility: staff can access data wherever they are, rather than having to remain at their desks.

Allows IT to Shift Focus: Not having to worry regarding constant server updates and varied computing issues. Government organizations unit progressing to be liberated to accept innovation. But at constant time there are a unit a unit some factors in cloud computing that has to be result on user, however at constant time there are a unit a unit a unit some factors in cloud computing that needs to be result on user.

Reliance on third Party: management over own data is lost at intervals the hands of associate “difficult-to-trust” supplier. Cost of transition: Is it realizable on behalf of yank state to maneuver from this kind of my info center to the planning of the cloud?

II. LITRETURE SURVEY

A literature review is an evaluative report of information found in the literature related to selected area of study.

a) "Reliable Delivery and Filtering for Syslog" first published in the year 2006. This permits a tool to be made-to-order for receipt of syslog messages. This feature provides reliable and secure delivery for syslog messages victimization Blocks extensile Exchange Protocol (BEEP). To boot, it permits multiple sessions to one work host, freelance of the underlying transport methodology, and provides a filtering mechanism named as a message individual. This module describes the functions of the Reliable Delivery and Filtering for syslog feature and thus the due to be a part of them throughout a network.

b) Karen Kent Murugiah Souppaya in the year 2006 has developed "Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology". It provides sensible, real-world steering on developing, implementing, and associated maintaining effective log management practices throughout an enterprise. The steering throughout this publication covers many topics, at the side of establishing log management infrastructures, and developing and enjoying strong log management processes throughout a company. The publication presents log management technologies from a high-level viewpoint, and it's not a stepwise guide to implementing or exploitation log management technologies.

c) Sebastian Schmerl, archangel Vogel, René Rietz, and Hartmut König Computer Networks and Communication Systems cluster Brandenburg University of Technology, Cottbus, Germany worked on "Explorative Visualization of Log Data to support Forensic Analysis and Signature Development ” in the year 2010. In this paper, we've got an inclination to tend to propose Associate in nursing approach for log resp. audit information illustration that aims at simplifying the analysis technique for the protection officer. For this purpose audit information and existing relations between audit events square measure pictured diagrammatically throughout a 3 dimensional area. We’ve got an inclination to tend to clarify a general approach for analyzing and exploring audit or log information within the context of this presentation paradigm. Further, we've got an inclination to tend to introduce our tool, that implements this approach and demonstrate the strengths and edges of this presentation and exploration kind.

d) "On the Security of Public Key Protocols" developed by DANNY DOLEV AND saint c. YAO, MEMBER, IEEE. The Use of public key secret writing to provide secure network communication has received tidy attention. Such public key systems square measure typically extremely effective against a “passive” spy, namely, one WHO simply faucets the communication line and tries to decipher the intercepted message. However, as detected in Needham associated Schroeder associate improperly designed protocol can be vulnerable to associate “active” saboteur, one who might impersonate another user and might alter or replay the message. As a protocol can be compromised terribly} terribly tough implies that, informal arguments that assert the protection for a protocol unit susceptible to errors.

e) In the year 1985 "Architecture of an Open Object-Oriented Database Management System" developed by David L. Wells, Jose A. Blakeley, and Craig W. Thompson TX Instruments. The Use of public key secret writing to provide secure network communication has received tidy attention. Such public key systems are typically extremely effective against a “passive” spy, namely, one who simply faucets the communication line and tries to decipher the intercepted message. However, as detected in Needham associated Schroeder associate improperly designed protocol can be vulnerable to associate “active” saboteur, one WHO might impersonate another user and might alter or replay the message. As a protocol can be compromised terribly} terribly tough implies that, informal arguments that assert the protection for a protocol unit susceptible to errors.

f) "Concurrency Control in Distributed Object-Oriented Database Systems" developed by Kjetil Norvag, Olav Sandsta, and Kjell Bratbergsengen in 1997. Department of laptop computer and information Science, Norwegian University of Science and Technology.In this paper we've got given results from simulations with 2 absolutely wholly completely different hardware methods. Any work for the DBsim machine includes extensions that will manufacture it ample acceptable for simulation of algorithms for object-oriented databases. Obviously, way more square measure aiming to be finished each the simulation model and to boot the machine. This includes adding new schedulers to the system, e.g., completely different versions of the two-phase protection hardware, like wound-wait and wait-die. In associate very real system, replication is used for inflated responsibility and performance. this may probably even be integrated into this framework.

III.EXISTING SYSTEM

To achieve secure data sharing in the cloud, we expect to combine the signature and encryption techniques.The signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption**.**Technique allows data owners to securely share their data files with others including new joining users.

LIMITATIONS:

- The computation overhead of users for encryption operations and the cipher text size are constant
- The encryption policy is described in the keys, so the encrypted does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users
- There is no log management.

IV. PROPOSED WORK

In this paper, We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user’s credentials. Key distribution is done in a decentralized way. And we hide the attributes and access policy of a user. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify the data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud

ADVANTAGES:

- A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext.
- User Revocation
- Secure log Management.

DOI: 10.15680/IJIRCCE.2016. 0408074

V. MODULES

a) Log Generator:

These are the computing devices that generate log data. Each organization has adopts the cloud-based log management service has a number of log generators. Each of these generators is up to with logging capability. The log files generated by these hosts are not stored locally except temporarily till such time as they are pushed to the logging client.

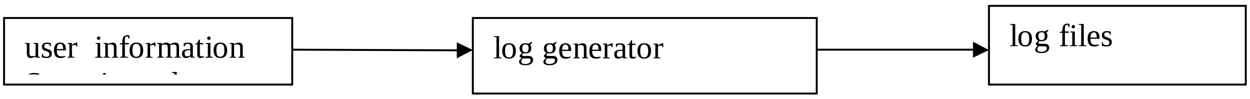

Fig: 1 Log generator

b) Logging Client:

The logging client is a collector that receives groups of log records generatedby one or more log generators, and prepares the log data so that it can be pushed to the cloud for long term storage. The log data is transferred from the generators to the client in batches, either on a schedule, or as and when needed depending on the amount of log data waiting to be transferred. The logging client incorporates security protection on batches of accumulated log data and pushes each batch to the logging cloud. When the logging client pushes log data to the cloud it acts as a logging relay. We use the terms logging client and logging relay interchangeably. The logging client or relay can be implemented as a group of collaborating hosts. For simplicity however, we assume that there is a single logging client.

.

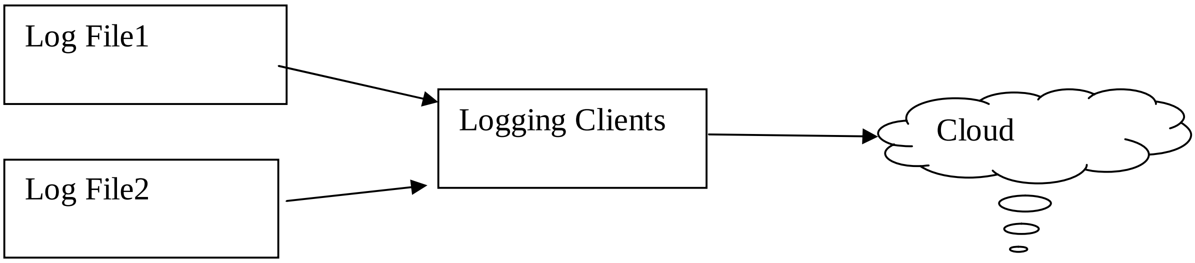

Fig: 2 Logging Clients

c) Logging Cloud:

The logging cloud provides long term storage and maintenance service to log data received from different logging clients belonging to different organizations. The logging cloud is maintained by a cloud service provider. Only those organizations that have subscribed to the logging cloud's services can upload data to the cloud. The cloud, on request from an organization can also delete log data and perform log rotation. Before the logging cloud will delete or rotate log data it needs a proof from the requester that the latter is authorized to make such a request. The logging client generates such a proof. However, the proof can be given by the logging client to any entity that it wants to authorize.

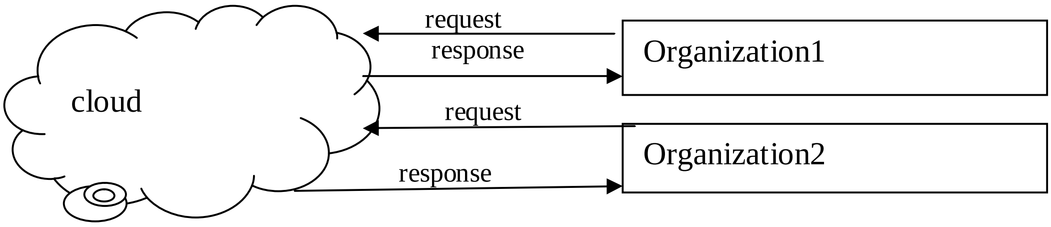

Fig: 3 Logging Cloud

d) Log Monitor:
These are hosts that are used to monitor and review log data. They can generate queries to retrieve log data from the cloud. Based on the log data retrieved, these monitors will perform further analysis as needed. They can also ask the log cloud to delete log data permanently, or rotate logs.

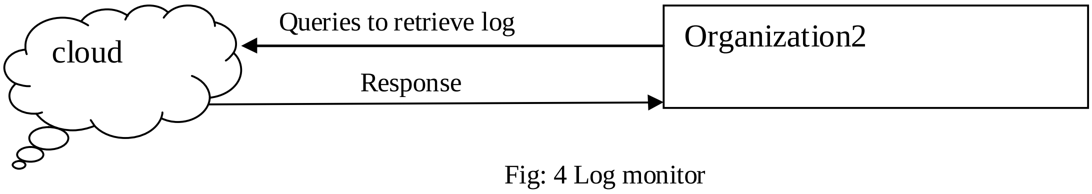

Fig: 4 Log monitor

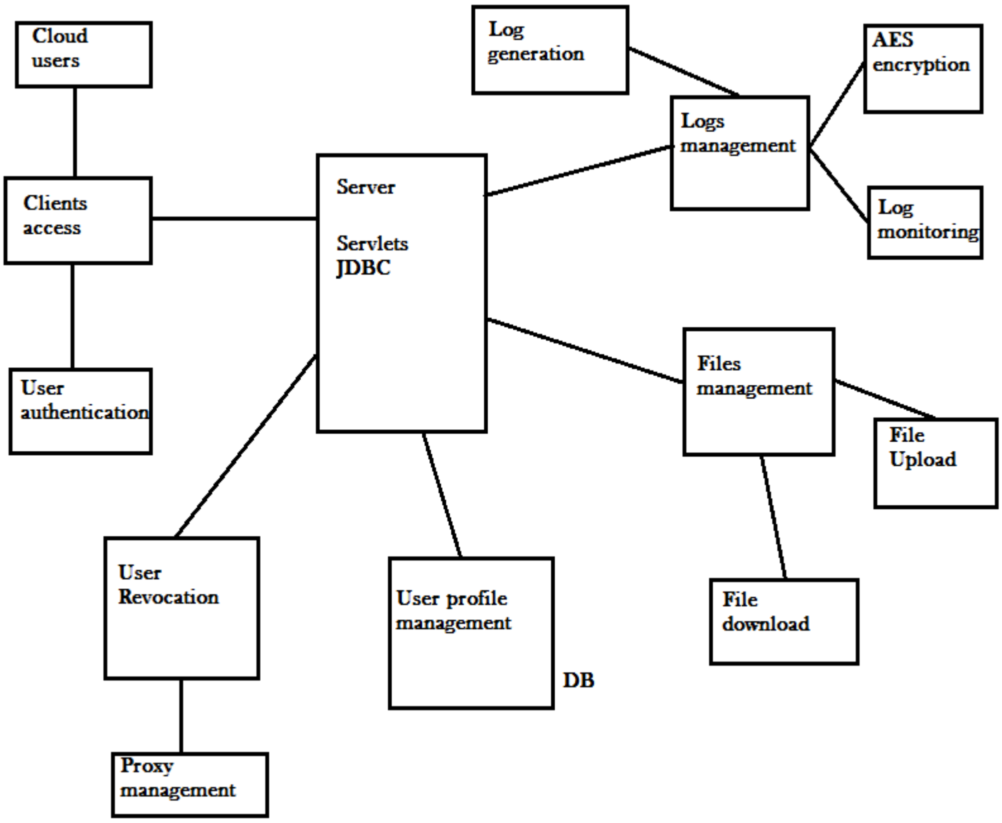

Fig: 5 Architectural Diagram

VI. CONCLUSION

We have presented a anonymous access control. And projected a full system to firmly give log records to a cloud provide, user revocation process and full secure for the cloud storage. In this paper we use Attribute based access control. And secutity is provided to logs, So only authorised person can access the cloud and by using the logs we can revocate the user for misbehaviour.

VII. TEST AND RESULTS

Test Case	Check Field	Objective	Expected Result
TC-001	User	Failed to open the application	Should check net connections
TC-002	User	Log in	Correct user name and password should enter
TC-003	User	Failed to login	Error means "not registered'
TC-004	User	To view the log	Enter the secret key which is send to user mail
TC-005	User	upload	After log in user can upload the file
TC-006	User	Dowload the file	Only authorised user can download the file
TC-007	User	While download and uploading	Logs are maintaned
TC-008	Admin	Revocation	Revocates the user for misbehaviour.

REFERENCES

[1] A.Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A.Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[4] J.Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V.Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.