ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Dynamic Auditing and Accounting Mechanism for Policy Based Data Access in Cloud

[1]P.Krubhala,[2]K.SaravanaKumar
[1] M.E. Second Year and [2] Assistant Professor,
Department of Computer Science and Engineering, V.S.B Engineering College, Karur

Abstract-Cloud computing is advancement in the field of information technology. The terminology cloud computing can be illustrated as pay-as-you-use model in which this framework includes collection task where they are assigned to the clients who needs it. Without the features of internet its impossible to provide a cloud environment. Lots of gain can be achieved through the cloud such as scalability, availability, flexible, lots of storage space, low cost and so on. Although it embraces these benefits the major venture of cloud technology is that security and confidential of data stored and shared within or between the third party environment. In order to overcome these problem the audit ability scheme can be endowed where this methodology supports to check the integrity of the data being stored and allows for the user data privacy. Further our work also proposes the accounting mechanism for metering the resource usages where the system encloses user data along with their policies. The result of accounting mechanism is the generation of the log record.

Index terms: **Accounting, Auditing, Integrity**

I. INTRODUCTION

Cloud computing is an environment where software applications, processing power, data and potentially even artificial intelligence are accessed over the Internet. Many private exchanging messages and sharing photos and video on social networking sites like Face book is very common [11].However, these types of cloud computing activities are just the beginning. Indeed, it is likely that within a decade the vast majority of personal and business computing will be Internet based which is the backbone of cloud. Cloud computing is dynamically scalable because users only have to consume the amount of online resources they actually want. Just as we are used to drawing as much or as little electricity as we need from the power grid, so anybody can now obtain as many or as few computing resources from the cloud as they require at any particular point of time.

One of its major disadvantages is the security related issues where users fear of losing the control over their own data. To overcome this problem there is needs for auditing the resources which is being stored in the third party environment and monitor the usage of resources by using accounting schemes. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. The another major issue in cloud is the cloud service providers. The cloud service providers can be described as a person or an organization which is responsible for making a service available to interested parties. A Cloud provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services and makes arrangement to deliver the cloud services to the cloud consumers through network access [24].The following are the major disadvantages of CSP [25]

- No influence on maintenance levels and fixes frequency when using cloud services from a CSP.
- No or little insight in CSP contingency procedures. Especially backup, restore and disaster recovery.
- Measurement of resource usage and end user activities lies in the hands of CSP.
- No easy migration to another CSP.

The solution for the above challenges can be achieved by using an approach named Secured Cloud Accountability framework[1].Information accountability allows for hide-it-or-lose-it perspective where our proposed framework supports end-to-end accountability in a distributed manner. The Secure cloud accounting framework conforms the security of data being send to the cloud storage by using the Cipher text policy based encryption [15].In addition to the above security features the framework also permits to monitor the usage of data. The usage of data can be tracked based on the service level agreements beside with this characteristic the service level agreements can be updated dynamically. Related to the accountability feature, the framework also

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

includes the TPA which performs the auditing of the data being in the cloud storage. This system encourages public auditing by proposing a protocol which enables dynamic data operation to support block insertion.

II.RELATED WORK

The succeeding section gives an overview about various security and privacy issues related to cloud.

A .Issues related to privacy

Remote data integrity checking is a protocol that focuses on how frequently and efficiently we verify whether cloud server can faithfully store the user's data without retrieving it [4]. The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud [5].Data leakages out of cloud computing environments are fundamental cloud security concerns for both the end- users and the cloud service providers. An effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure-correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques [6]. A data protection scheme with public auditing scheme is outlined that will address a number of these factors, by providing a mechanism to allow for data to be encrypted in the Cloud without loss of accessibility or functionality for authorized parties. This scheme is not necessarily a replacement for traditional privacy and security measures for data [7]. For cloud computing services to become successful and sustainable, we need a systematic framework for verifiable resource accounting. It eases any concerns that customers may have with providers' pricing and performance guarantees. It also gives customers a basis for accurately comparing different cloud providers [8].

B.Other issues in maintaining privacy

Privacy and security in the cloud denotes a big challenge. By encrypting the data it strengthens the security already in place though the cloud. Through encryption you also have a means of ensuring your data can be destroyed if necessary. Risk management of the data throughout its life cycle is crucial[9].The newly proposed scheme, doesn't allow user's rating to stored in the cloud. Our scheme does not rely on any trusted third party for threshold decryption by allowing the users to encrypt and decrypt a prediction query and its results respectively. The results shows that the user can obtain predictions quickly despite encrypted rating queries [12].A new cryptographic framework that can protect data both in cloud storage and cloud-based applications. The implementation of such a framework enables users to enjoy the tremendous benefits of cloud services while at the same time having their data protected [13]. Any TPA in possession of the public key can act as a verifier. We assume that TPA is unbiased while the server is untrusted. For application purposes, the clients may interact with the cloud servers via CSP to access or retrieve their pre-stored data. More importantly, in practical scenarios, the client may frequently perform block-level operations on the data files.

III.SECURE CLOUD FRAMEWORK

The security of the cloud environment can be improved by means of allowing both the accounting and auditing information to the data owners. Let's discuss about the features of this framework.

A. Key factors of Cloud framework

The construction of the framework involves diverse of components such as the data, users, logger and harmonizer.

*Data:*In cloud environment data can be an image, text files, documents and so on.

Users: The users are the consumers of cloud services.

Logger: The logger is the component which is strongly coupled with the user's data, so that it is downloaded when the data are accessed, and is copied whenever the data are copied.

Third party auditor: The auditing function is handled by the TPA which is an external auditor. It provides the auditing message as the result to the data owners.

B.Proposed work

The basic flow of the operation is shown in the figure 1.The secure cloud framework allows for both the metering and auditing of the resources. The accounting services measures the performance and consumption of the resources which helps for optimize cloud service delivery [14]. In addition to the accounting services this framework also includes an auditing mechanism. Its intention is to increase the level of security.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

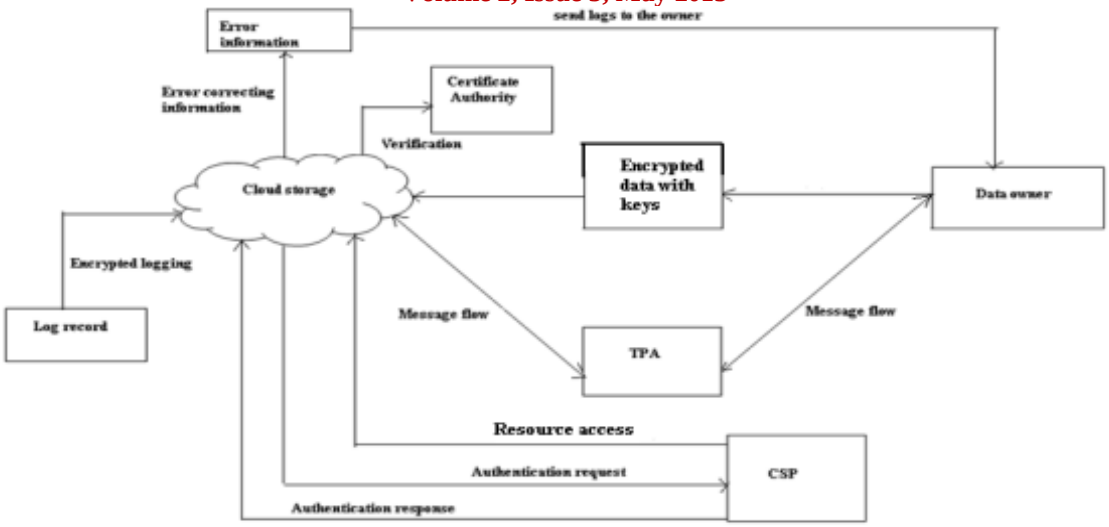

Fig 1 Secured cloud framework architecture

A third party auditor is responsible for performing the auditing. The Cloud Audit is responsible for cloud service providers with a way to make their performance and security data readily available for potential customers. The specification provides a standard way to present and share detailed, automated statistics about performance and security [15].

IV.ACCOUNTING MECHANISM

The first phase is to implement the accounting mechanism where it is described as follows. Initially each owner of the resources encrypts their data using the Cipher text policy based encryption [16]. This encryption doesn't need any third party to provide the encrypted data that is no need of generate the key and encrypt. In this mechanism an encryptor express the access policy where it decides what kind of recovers can decrypt the original information. These kind of access policies are stated as the service level agreements in cloud environment [1].Whenever an SLA is formed, the level of risk incurred is based on how well the offered service terms meet the organizational security demands. At runtime, whenever a cloud or service violates its SLA with respect to security controls or cancels any security offerings, the risk of noncompliance with organizational security policies increases[17].The encrypted data is now stored in logger component along with their service level agreements. The access policies along with the JAR file is send to the CSP.The authenticity of the CSP is provided based on the SAML based certificate authority [26].This trusted identity provider issues certificates verifying the user's identity based on his username. Only after the completion of authentication succeeds the users or service provider is made to access the data enclosed with JAR file. As for the logging, each time there is an access to the data, the JAR will automatically generate a log record, encrypt it using the public key distributed by the data owner, and store it along with the data. The encryption of the log file prevents unauthorized changes to the file by attackers.

A. Log record generation

Log records are generated by the logger component. Logging occurs at any access to the data in the JAR, and new log entries are appended sequentially, in order of creation LR ¼ hr1; . . . ; rki.Each record r_i is encrypted individually and appended to the log file. In particular, a log record takes the following form:

$$R_{i=}(ID,Act,T,Loc,h((ID,Act,Loc,)|r_{i-}1|\ldots|r_1),sig)$$

to the checksum of the records preceding the newly inserted one, concatenated with the main content of the record itself. The checksum is computed using a collision-free hash function [27].The component sig denotes the signature of the record created by the server. This type of log record ensures the accounting feature to the data owner and allows checking whether their datas are handled according to the service level agreements.

V.AUDITING MECHANISM

The next phase of our work is performing an efficient auditing mechanism where it assures the integrity of the data being stored in the cloud. To audit the cloud environment we need a third party auditor. The external auditor supports that the cloud provider is constantly following policies, procedures and processes, which are defined by the customer, to meet their business requirements.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

A. Auditors role

The audit functions can be handed over to a third party whom the customer as well as provider trusts. Before conducting audits on a cloud, the customer must identify what are the expectations of his/her internal audit department and what are the expectations of the external auditor with respect to meeting the internal expectations.To implement a third-party audit for cloud computing operations, the owner of the data must set up a private key and a public key. The private key allows total access to the data stored in the cloud. The public key allows access to certain blocks of data that the independent verifier will use to test the security, integrity and vulnerability of the data stored. The verifiers can detect modifications, corrupt files and deletions [10].

B. Protocol proposed

An effective public auditability protocol is proposed to ensure the data integrity. Along with that dynamic data operation is allowed to the clients to perform block-level operations on the data files while maintaining the same level of data correctness assurance [3].

C.Auditing protocol

To implement the public auditing mechanism the data being used is to be segmented as blocks to verify the integrity. In order to divide these files into blocks the Merkle hash tree is being used. The main functionality of this to allow efficient and secure verification of the contents of larger data structure. It is constructed as a binary tree where the leaves in the MHT are the hashes of authentic data values[3].MHT is commonly used to authenticate the values of data blocks.

The receiver knows the public key pub, the message M,and the signature sig=(sig′||$auth_0$||$auth_1$||...||$auth_{n-1}$). At first, the receiver verifies the one-time signature sig′ of the message M. If sig′ is a valid signature of M, the receiver computes A_0=H(Y_i) by hashing the public key of the one-time signature. For j=1, ..,n−1, the nodes of Aj of the path A are computed with Aj=H(a_{j-1}||b_{j-1}). If An equals the public key pub of the merkle signature scheme, the signature is valid[18].

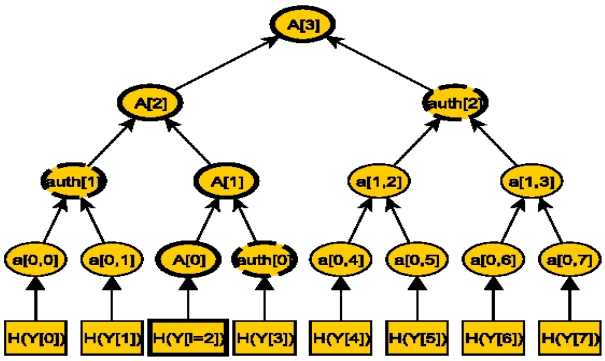

Fig 2 Merkle hash tree

D.Key terms

The execution of the algorithm can be justified by using the following key terms.

Setup: The client's public key and private key are generated by invoking KeyGen(.).By running SigGen(.),the data file F is pre processed, and the homomorphic authenticators together with metadata are produced.

*KeyGen(1^k):*The client generates a random signing key pair(spk,ssk).Choose a random α←Zp and compute v←gα.The secret key issk= (α,ssk) and the public key is pk=(v,spk)

SigGen(sk,F): Given F= (m_1,m_2 ...,m_n), the client chooses a random element u←G.Let t=name||n||u|| SSigssk(name||n||u) be the file tag for F. Then the client computes signature σi for each block mi(i= 1,2,...,n) as σi←(H(mi). $u^{m}{}_{i}$)$^{\alpha}$.Denote the set of signatures by Φ ={σi},1≤i≤n.The client then generates a root R based on the construction of Merkle Hash Tree (MHT), where the leave nodes of the tree are an ordered set of hashes of "file tags" H(mi) (i= 1,2,...,n).Next, the client signs the root R under the private key α:sig_{sk}(H(R))←(H(R))α.The client sends {F,t,Φ,sigsk(H(R))} to the server and deletes {F,Φ,sigsk(H(R))}from its local storage .

E.Default Integrity Verification

The client or TPA can verify the integrity of the outsourced data by challenging the server. Before challenging, the TPA first use spk to verify the signature on t.If the verification fails, reject by emitting FALSE ;otherwise, recover u .To generate the message " chal ", the TPA (verifier) picks a random c element subset I ={ s_1,s_2 ,...,s_c} of set[1,n], where we assume $s_1 \leq \ldots \leq s_c$. For each i ∈ I the TPA chooses a random element v_i←B ⊆ Zp. The message"chal" specifies the positions of the blocks to be checked in this challenge phase.The verifier sends the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

chal{(i,v_i)} $s_1 \le i \le s_c$ to the prover (server). GenProof(F,Φ,chal).Upon receiving the challenge chal={(i,v_i)}$s_1 \le i \le s_c$,the server computes

$$\mu = \sum_{i=s_1}^{s_c} v_i m_i \in Z_p \text{ and } \sigma = \prod_{i=s_1}^{s_c} \sigma_i^{v_i} \in G_i$$

where both the data blocks and the corresponding signature blocks are aggregated into a single block, respectively. In addition, the prover will also provide the verifier with a small amount of auxiliary information $\{\Omega_i\}s_1 \le i \le s_c$, which are the node siblings on the path from the leaves$\{h(H(m_i))\}s_1 \le i \le s_c$ to the root R of the MHT. The prover responds the verifier with proof $P=\{\mu,\sigma,\{H(m_i),\Omega_i\}s_1 \le s_c, sig_{sk}(H(R))\}$

F.Verify proof{P_k,chal,P}

Upon receiving the responses from the prover, the verifier generates root R using $\{H(m_i),\Omega_i\}s_1 \le i \le s_c$ and authenticates it by checking $e(sig_{sk}(H(R)),g) \stackrel{?}{=} e(H(R),g^{\alpha})$.If the authentication fails, the verifier rejects by emitting FALSE. Otherwise the verifier checks

$$e(\sigma,g) \stackrel{?}{=} e(\prod_{i=s_1}^{s_c} H(m_i)^{v_i}.u^{\mu},v)$$

If so, output TRUE ; otherwise FALSE. The protocol is illustrated as follows.

Table 1 Protocol proposed

TPA	CSS
1.Generate random set $\{i,v_i\}_{i \in I}$	
$\{(i_1,v_i)\}_{i \in I}$ → challenge request chal	
	2.Compute $\mu=\sum_i v_i m_i$
	3.Compute $\sigma=\prod_i \sigma_i^{v_i}$
$\{\mu,\sigma,\{H(m_i),\Omega_i\}_{i \in I},sig_{sk}(H(R))\}$ ← Integrity proof	
4. Compute R using $\{H(m_i),\Omega_i\}_{i \in I}$	
5.Verify $sig_{sk}(H(R))$ and	
Output FALSE if fails	
6.Verify$\{m_i\}_{i \in I}$	

G.Ensuring Integrity of data when modified

Now we show how our scheme can explicitly and efficiently handle fully dynamic data operations including data modification (M), data insertion (I) and data deletion (D) for cloud data storage. Note that in the following descriptions, we assume that the file F and the signature Φ have already been generated and properly stored at server. The root metadata R has been signed by the client and stored at the cloud server, so that anyone who has the client's public key can challenge the correctness of data storage.

H.Data Deletion

Similar to insertion deletion is the complex one. If there is a need to delete single block, it refers to deleting the specified block and moving all the other blocks one block forward. Suppose the server receives the update request for deleting block mi, it will delete m_i from its storage space, delete the leaf node h(H(mi)) in the MHT and generate the new root metadata R.

I. Batch Auditing for Multi-client Data

Since cloud servers concurrently handle multiple clients the verification process being done is also handled as multiple verification sessions. Lets consider K signatures on K distinct data files from K clients, it is more easier

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

to aggregate all these signatures into a single one and verify it at one time. The key idea is to use the bilinear aggregate signature scheme [28]. As in the BLS based construction, the aggregate signature scheme allows the creation of signatures on arbitrary distinct messages. Moreover, it supports the aggregation of multiple signatures by distinct signers on distinct messages into a single short signature, and thus greatly reduces the communication cost while providing efficient verification for the authenticity of all messages.

VI.RESULTS

The implementation of the secure cloud framework can be explained as follows.Initially the Secured Cloud Framework is shown which includes the auditing and accounting mechanism.

Fig 3 Secure cloud accounting and auditing framework

The next step is to include the user's task such as upload, download, search a file, delete a file and authentication for the data being stored in the cloud storage server.

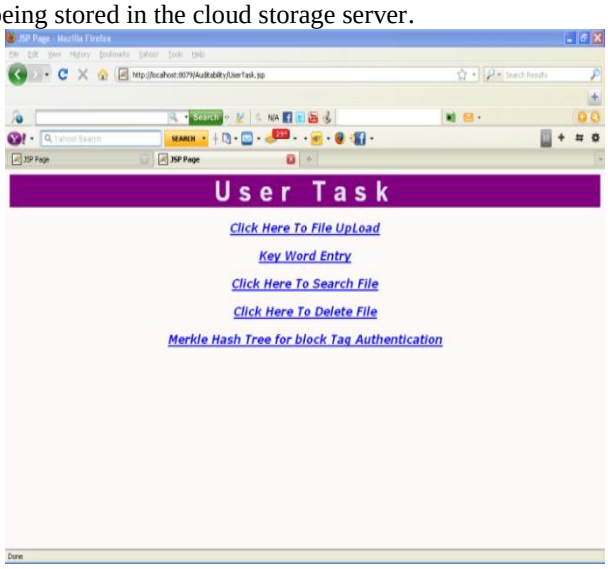

Fig 4 Tasks performed by users

Each time when there is a need for authentication it can be performed by providing the key values. The authentication is performed as block tag process.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Fig 5 Merkle block tag authentication

For dynamic updation of the data's the insertion and deletion of block is allowed.

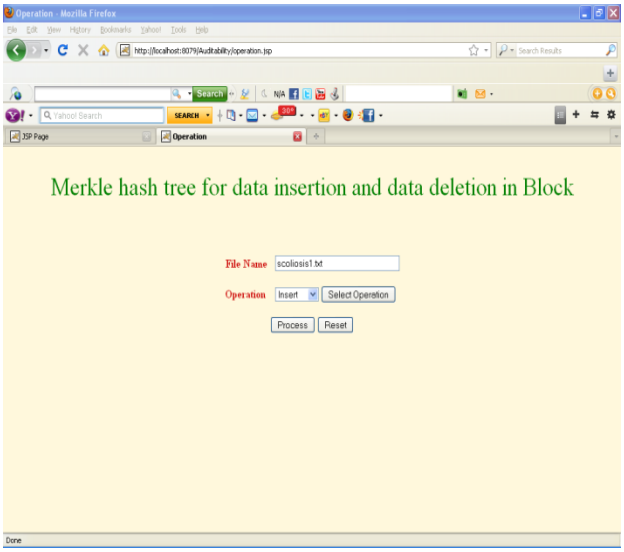

Fig 6 Dynamic updation

When the updation is finished then it allows the server to indicate the result of the auditing mechanism. It includes all the details about the updation.

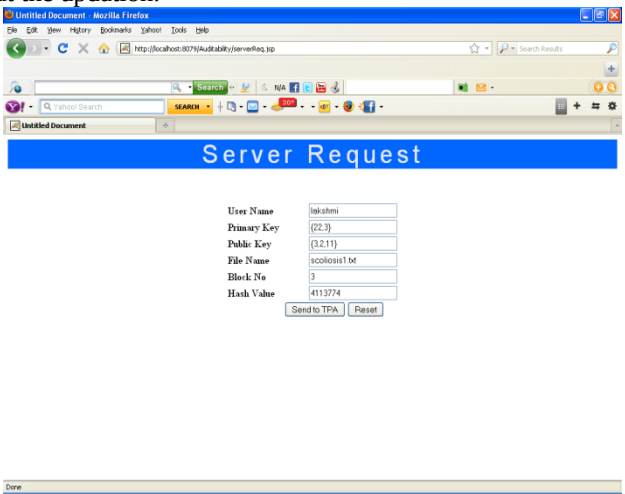

Fig 7 Server process

Now the third party is allowed to perform the auditing and the result is being provided.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

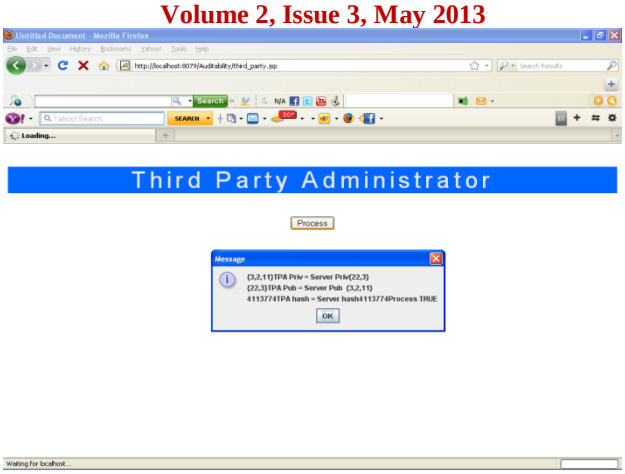

Fig 8 TPA auditing

Finally the information of resource usage is obtained by the data owner by the accounting mechanism.

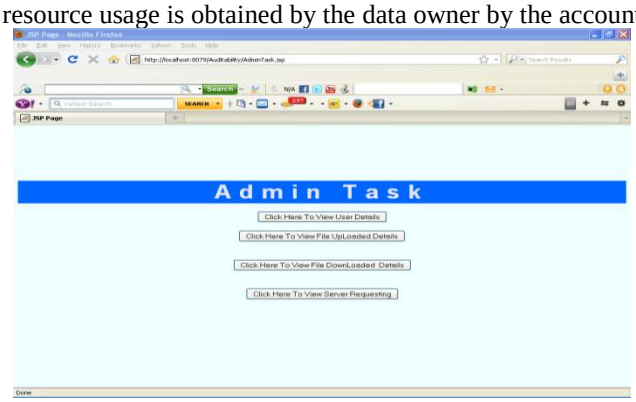

Fig 10 Generation of the log record

VII.CONCLUSION

The assurance cloud security is achieved by imposing both the auditing and accounting features. This are the major two features considered to solve the security related issues in cloud. Finally we achieved the monitoring process in cloud environment by proposing an efficient accounting mechanism which generates the log record as the result of the accounting function. In addition to that it increases the level of security by allowing the data owners to specify their service level agreements which are the contract between the service providers and users to maintain their data secure. To improve the level of security the proposed work also allows verifying the integrity of the cloud storage. This can be achieved on the basis of allowing a third party auditor to audit the data and also it supports for the batch auditing and dynamic modification of the data in the cloud.

REFERENCES

[1] Sundareswaran,S.Coll of Inf. Sci. & Techno., Pennsylvania State Univ., University Park, PA, USA Squicciarini, A.C.; Lin.D "Ensuring Distributed Accountability for Data Sharing in the Cloud"IEEE Transactions on in Dependable and Secure Computing, July-Aug. 2012.

[2] S. Sundareswaran, A. Squicciarini, D. Lin, and S.Huang, "Promoting Distributed Accountability in the Cloud," Proc. IEEEInt'l Conf. Cloud Computing, 2011.

[3] QianWang Dept. of Electr. & Comput. Eng., Illinois Inst. of Techno., Chicago, IL, USA Cong Wang; Kui Ren; Wenjing Lou; Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing "in IEEE Transaction in Parallel and Distributed Systems,May2011 Volume: 22 , Issue: 5 .

[4] Syam Kumar P, Subramanian R "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing" in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[5] Richard Chow, Philippe Golle, Markus Jakobsson,Ryusuke Masuoka, Jesus Molina Elaine Shi, Jessica Staddon PARC Fujitsu Laboratories of America" Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control" @parc.com@us.fujitsu.com,2010.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

[6] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology Email:{cwang, qwang, kren}@ece.iit.edu Wenjing Lou Department of ECE Worcester Polytechnic Institute Quality of Service," Ensuring Data Storage Security in Cloud Computing" in IWQoS. 17th International Workshop on 13-15 July 2009.

[7] Gowrigolla, B. Sivaji, S. Masillamani," Design and auditing of Cloud computing security" in 5th International Conference on Digital Object Identifier: 10.1109/ICIAFS.2010.5715676 Publication Year: 2010, Page(s): 292 – 297.

[8] Vyas Sekar Intel Labs Petros Maniatis Intel Labs" Verifiable Resource Accounting for Cloud Computing Services" CCSW'11, October 21, 2011, Chicago, Illinois, USA.

[9] http://www.windowsecurity.com/articles tutorials/Cloud_computing/Key-Cloud-Privacy-Concerns-2012.html.

[10] http://wiki.answers.com/Q/How_does_third_party_auditing_work_in_cloud_computing&altQ=How_Third_Party_Auditing_Work_In_Cloud_Computing.

[11] http://www.ukessays.com/essays/data-analysis/hands-of-data-security-in-cloud.php.

[12] Basu, A. Grad. Sch. of Eng., Tokai Univ., Tokyo, Japan Vaidya, J.; Kikuchi, H.; Dimitrakos, Theo" Privacy-preserving Collaborative Filtering for the Cloud" in Cloud Computing Technology and Science (Cloud COM), 2011 IEEE Third International Conference on Nov. 29 2011-Dec.2011.

[13] Mohd Rizuan Baharon,Qi Shi, David Llewellyn-Jones, Madjid Merabti School of Computing & Mathematical Sciences Liverpool John Moores University Liverpool, United Kingdom M.R.Baharon@2011.ljmu.ac.uk, {Q.Shi, D.Llewellyn-Jones, M.Merabti}"Enhancing Security of Data and Their Related Processing in Cloud Computing" in The 13th Annual Post Graduate Symposium on the Convergence Of Telecommunications, Networking and Broadcasting,2012, [14]http://cloudamize.tumblr.com/post/35874767398/understanding cloud monitoring

[14] http://searchcloudsecurity.techtarget.com/definition/CloudAudit[16]Yanli Ren Sch. of Commun. & Inf. Eng., Shanghai Univ., Shanghai, China Shuozhong Wang ; Xinpeng Zhang ; Zhenxing Qian "Fully Secure Cipher text-Policy Attribute-Based Encryption with Constant Size Cipher text ",2011.

[15] Hale, Matthew L. Tandy School of Computer Science, University of Tulsa, Tulsa, OK, USA Gamble, Rose "Risk propagation of security SLAs in the cloud" in Globe COM Workshops (GC Wkshps), and 2012 IEEE Dec. 2012.

[16] Georg Becker"Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis".

[17] Tebaa, M. Dept. of Math. & Comput. Sci., Univ. Mohammed V - Agdal, Rabat, Morocco El Hajji, S.; El Ghazi, A."Homomorphic encryption method applied to Cloud Computing" in Network Security and Systems (JNS2), 2012 National Days of 20-21 April 2012.

[18] JongyoulPark Electron. & Telecommun. Res. Inst.,Daejeon, South Korea Seungyun Lee "Privacy preserved entrust mechanism in cloud computing environment " in Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on Nov. 29 2011-Dec. 1 2011.

[19] Long Chen Inst. of Comput. Forensics, Chongqing Univ. of Posts & Telecommun., Chongqing, China Hongbo Chen"Ensuring Dynamic Data Integrity with Public Auditability for Cloud Storage "in Computer Science & Service System (CSSS), 2012 International Conference 11-13 Aug. 2012.

[20] Yong-jun, Geng Department of Computer Science and Engineer Henan University of Urban Construction Pingdingshan, China Jun-feng, Zhang"A new multi-signature scheme based on bilinear pairs "in International Conference on E -Business and E -Government (ICEE), 2011.

[21] Wenjun Luo Coll. of Comput. Sci. & Technol., Chongqing Univ. of Posts & Telecommun., Chongqing, China Guojing Bai "Ensuring the data integrity in cloud data storage " in Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on 15-17 Sept.2011.

[22]]NIST Special Publication 500-293,at 20-21.

[23] http://.cloudcomputingtechie.com/top-5-disadvantages/

[24] OASIS Security Services Technical Committee, "Security Assertion Markup Language (saml) 2.0," http://www.oasis-open.org/ committees/tc home.php?wg abbrev=security, 2012.

[25] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1993.

[26] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of Accountability and Audit," Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 152-167, 2009.