Customized Audit Approach to Achieve User Desired Control over Cloud Data

K. Karthik
Lecturer, Department of C S E
JNTUK, Kakinada
Kakinada. E.G.Dt., A.P. India.
kkarthik46@gmail.com

D. Meenu
Asst Professor, Department of C S E
Ideal Engg college, Kakinada
Kakinada. E.G.Dt., A.P. India.
meenudonka@gmail.com

Abstract: Cloud computing is the mainly used technique in the modern days in order to avoid the problems in the storage of the data in online to access the data from anywhere. In this paper, traditionally we will be utilizing a method based on probabilistic query and periodic verification for improving the performance of audit services. By using these methods, we will be improving the effectiveness of verification of storage data and decrease the storage space for extra data. There will not be any user-desired control in the data retrieval provided by these methods. Therefore, to overcome this problem we will be using object-centered method that enables enclosing our logging mechanism collectively with user's data and policies. To support user's control, we also present distributed auditing mechanisms by which we will be observing efficiency and the effectiveness of the proposed approach.

Keywords: *Probabilistic query, Periodic verification, Object-centered method, distributed auditing.*

*****

I. INTRODUCTION

Cloud computing is computing that include a large number of computers connected through a communication network such as the Internet, similar to utility computing [4]. In science, cloud computing is a synonym for distributed computing over a network, and means the skill to run a program or application on many connected computers at a time. Network-based services, which appear to be delivered by real server hardware and are in fact served up by virtual hardware replicated by software running on one or more real machines, is often called cloud computing. Such replicated servers do not physically exist and can therefore be relocated around and scaled up or down on the fly without disturbing the end user, somewhat like a cloud becoming larger or smaller without being a physical object [3].

The major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service [3].

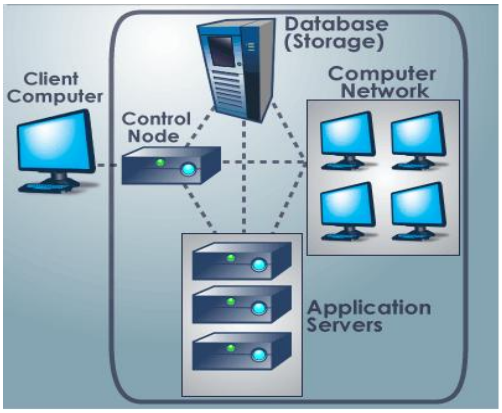

Fig-1.Overview of cloud computing

In general usage, the term "the cloud" is fundamentally an allegory for the Internet [5]. Marketers have further made popular the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. remotely through the Internet. Typically, the seller has actual energy-consuming servers that host products and services from a remote location, so end-users do not have to; they can simply go through the network without installing anything.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility over a network [6]. At the foundation of cloud computing is the wide concept of converged infrastructure and shared services. The cloud also concentrates on maximizing the effectiveness of the shared resources. The Cloud resources are not habitually only shared by multiple users but they are also dynamically reallocated per demand. This can work for allocating resources to users.

Auditing in the cloud computing will be mainly helpful for the effective and efficient resource delivery which will be helpful to users in order to easily access the data that is present inside the cloud. Cloud computing will be presenting a new enhances the current consumption and providing of IT services which are based on internet. Details of the services provided are abstracted from the users who no longer need to be experts of technology infrastructure.

Therefore, following performance objectives should be addressed to achieve an efficient audit for outsourced storage in clouds:

- **Public auditability**: To allow a third party auditor (TPA) or clients with the help of TPA to verify the

correctness of cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to cloud services;

- **Dynamic operations**: To ensure there is no attack to compromise the security of verification protocol or cryptosystem by using dynamic data operations.
- **Timely detection**: To detect data errors or losses in outsourced storage, as well as anomalous behaviors of data operations in a timely manner;
- **Effective forensic**: To allow TPA to exercise strict audit and supervision for outsourced data, and offer efficient evidences for anomalies

II. RELATED WORK:

G. Ateniese stated that by introducing the provable data possession (PDP) that will be allowing the clients to verify the untrusted data that is stored in the servers and will be helpful for the effective retrieval of the data from the cloud. This model will be providing the proofs that will also be decreasing the I/O cost drastically. For the further enhancement of these, proposed system will be presenting two provably secure schemes. This will be more effective than the traditional methods used.

R.D. Pietro stated that storage outsourcing is a rising trend, which prompts a number of interesting security issues, many of which is been extensively investigated in the past. There is a main issue how to increase the frequently, efficiently and securely verify that a storage server is faithfully storing its client's. This problem is been solved by using the proposed technique where we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption.

D. Boneh stated that a fully functional identity-based encryption scheme (IBE) was proposed cipher text security in the random oracle model assuming an elliptic curve variant of the computational Diffie-Hellman problem is chosen by the scheme. Weil paring mainly based on this system. Precise definitions are given by the system in order to secure identity based encryption schemes and given many different applications helpful for the effective working.

B. Chun stated that here in the paper he will be discussing about three key problems for trust management in federal systems. Those problems will be including how to express and verify trust in a scalable and flexible manner. These problems will be closing the trust management and are especially in this context of federal systems. Where remote resources can be acquired across multiple administrative domains and used in potentially undesirable ways

R. Corin stated that a language that will be allowing agents to distribute data with usage policies in a decentralized architecture. The compliance with usage policies are not enforced in framework that is created by him. A logic that allows audited agents to prove their actions, and to prove their authorization to posses particular data that are designed. Several flavors, including agent accountability and data accountability are defined as a result. Soundness in logic is finally shown.

III. EXISTING SYSTEM

Audit system architecture will be mainly consisting of the owner of the data, authorized applications and users, data server and name server. All the process is shown in the below diagram. It will be giving the clear idea about whole process that is taken palace in audit system.

Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity who accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed.

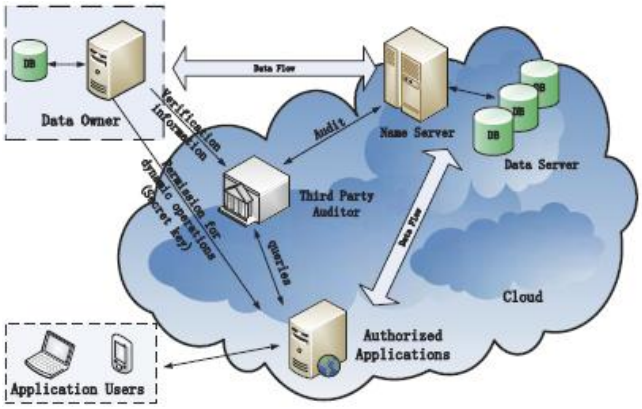

Fig-2.Architecture of Audit System.

There are many functions in this audit system and there will be comprised of three processes. They are

- Tag generation
- Periodic sampling audit
- Audit for dynamic operations

Tag generation: The client (DO) uses a secret key sk to preprocess a file, which consists of a collection of n blocks, generates a set of public verification parameters (PVPs) and index-hash table (IHT) that are stored in third party auditor (TPA), transmits the file and some verification tags to cloud service providers (CSP), and may delete its local copy.

Periodic sampling audit: By using an interactive proof protocol of retrievability, TPA (or other applications), issues a "random sampling" challenge to audit the integrity and

availability of the outsourced data in terms of verification information (involving PVP and IHT) stored in TPA.

Audit for dynamic operations: An AA, who holds a DO's secret key sk, can manipulate the outsourced data and update the associated IHT stored in TPA. The privacy of sk and the checking algorithm ensure that the storage server cannot cheat the authorized applications (AAs) and forge the valid audit records.

The audit operations are done will be according to the process that will be followed by the cloud but not the user. Therefore, to overcome this we will be introducing our proposed approach that will be giving the total control to the user and the functioning will be done according to the user's desire.

IV. PROPOSED SYSTEM:

We describe our distributed auditing mechanism including the algorithms for data owners to query the logs regarding their data.

PUSH AND PULL MODE:

Here in this method we will observe that push method and pull method will be conducted separately as 1. Push mode and 2. Pull mode.

Push mode

In this mode, the harmonizer periodically pushes the logs to the data owner (or auditor). Either type of the following two events will trigger the push action: one is that according to the temporal timer inserted as part of the JAR file or a certain time is elapsed; the other is that the size will be exceeding in the JAR file stipulated by the content owner at the time of creation. The log files will be dumped, after the logs are sent to the data owner, to free the space for future access logs. The error correcting information for those logs is dumped along with the log files. This push mode is the basic mode, which can be adopted by both the PureLog and the AccessLog, regardless of whether there is a request from the data owner for the log files. Two essential functions are served by this mode in the logging architecture: 1) it ensure that the size of the log files does not explode and 2) it enables timely detection and correction of any loss or damage to the log files. Concerning the latter function, we notice that the auditor, upon receiving the log file, will verify its cryptographic guarantees, by checking the records' integrity and authenticity. The auditor will be able to quickly detect forgery of entries, by constructing the records using the checksum added to every record.

Pull mode

This mode allows auditors to retrieve the logs anytime when they want to check the recent access to their own data. The pull message consists simply of an FTP pull command, which can be issues from the command line. For naive users, a wizard comprising a batch file can be easily built. The request will be sent to the harmonizer, and the user will be informed of the data's locations and obtain an integrated copy of the authentic and sealed log file.

Size: maximum size of the log file specified by the data owner, time: maximum time allowed to elapse before the log file is dumped, tbeg: timestamp at which the last dump occurred, log: current log file, pull: indicates whether a command from the data owner is received.

Algorithm:

1. Let TS(NTP) be the network time protocol timestamp
2. pull=0
3. rec:=(UID, OID, AccessType, Result, Time, Loc)
4. curtime:= TS(NTP)
5. lsize:= sizeof(log) // current size of log
6. if ((cutime -tbeg) < time) && (lsize < size)&&(pull == 0) then
7. log :=log + ENCRYPT(rec) // ENCRYPT is the encryption function used to encrypt the record
8. PING to CJAR // send a PING to the harmonizer to check if it is alive
9. **if** PING-CJAR **then**
10. PUSH RS(rec) // write the error correcting bits
11. **else**
12. EXIT(1) // error if no PING is received
13. **end if**
14. **end if**
15. **if** ((cutime - tbeg) > time) || (lsize >= size) || (pull ≠ 0) **then**
16. // Check if PING is recived
17. **if** PING-CJAR **then**
18. PUSH log // write the log file to the harmonizer
19. RS(log) := NULL // reset the error correction records
20. tbeg := TS(NTP) //reset the tbeg variable
21. pull :=0
22. **else**
23. EXIT(1) // error if no PING is received
24. **end if**
25. **end if**

The above algorithm will be explaining the process of auditing the cloud storage data clearly.

V. RESULTS:

In the results, we will be saying that we observe the traditional method is not allowing the all the functions that

will desire to do by the user and cannot get full access of the data in the cloud. So, this problem can be solved by the proposed approach, which will be yielding the effective and desired approach and will be giving the full access and control to the users as he can perform any sort of operation on the cloud.

VI. CONCLUSION:

We conclude that by using the traditional method, we will be getting the results but they will not be under the full control of the user's i.e., they cannot do all the operations required and desired. Therefore, by using the proposed approach we can get full control over cloud that what we can do according to the user's desired operation. Therefore, there are no drawbacks up to some extent by using the proposed approach to get the desired outputs.

REFERENCES:

[1] Ensuring Distributed Accountability for Data Sharing in the Cloud by Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin

[2] 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 Communication.

[3] Cloud computing from Wikipedia.

[4] Securing Virtual and Cloud Environments". In I. Ivanov et al. Cloud Computing and Services Science, Service Science: by Mariana Carroll, Paula Kotzé, Alta van der Merwe.

[5] Cloud Computing entry". By NetLingo.

[6] The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[7] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm).

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

[9] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS).

[10] R. Corin, S. Etalle, J.I. 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.

Authors

Karthik Kota received the M.Tech in Computer Science and Engineering in 2013 from Jawaharlal Nehru Technology University, Kakinada, India. Working as a Lecturer in Department of Computer Science and Engineering at Jawaharlal Nehru Technology University, Kakinada.

Meenu Donka received the M.Tech in Computer Science and Engineering in 2013 from Jawaharlal Nehru Technology University, Kakinada, India. Working as an Asst Professor in Department of Computer Science and Engineering at Ideal Engineering College, Kakinada.