ENSURING DISTRIBUTED ACCOUNTABILITY FOR DATA SHARING IN THE CLOUD

D. J. Bonde, Mahesh Zite, Sachin Hol, Sandip Shinde, Yogesh Wagh

Abstract

Cloud computing is present a new Technology to Share Data or IT Based Service over the internet. Cloud Service provider are basically used to handle data to the unknown type of resources [1].for sharing of data over the cloud also used more entities. Those entities are relevant with each other in the cloud. Also cloud computing technology is provided a approach of Dynamic data handling .But overcome to this method sharing of data over the cloud is complex process. So that for the solution of this we are use the new framework know as (CIA)Cloud Information Accountability[3].In the cloud Information Accountability, if any user are subscribe this type of service, then service provider should provide the Access control or rights. By using the Mechanism of Access control whole information will be stored in the service provider.CIA also consists of two measure part logger and log harmonizer. JARs are used to create the Dynamic object. Ensure to this if any user should Access such data or information it will automatically logging or Authentication to JARs [4].

---***---

1.INTRODUCTION

The Cloud Information Accountability (CIA) is consisting of Automated logging mechanism. It has categories two measure part: Logger and log harmonizer [3].

JAR files consist of the collection of the different rules in which different Authorization of Access should take place. Each separate logging should carry out through integrity checks. Created files are contain "Reed-Solomon-Based encoder" [4].

Creation of JARs - In the creation of JARs, when any user uploads their file, at that time JARs file is created automatically. JARs consist of one or more collection of JARs file. So that it is important method for security purpose.log file is consist of record of every JARs file [2]. Whenever any

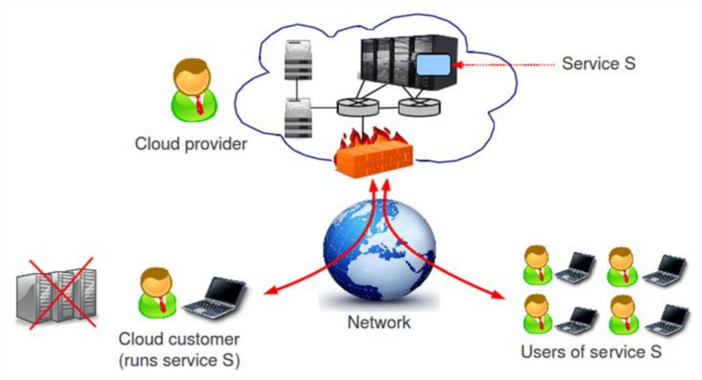
Technical problem cause or Damage log file, that log file are Restored through the Recovery Mechanism.
Certificate Authority- Certificate Authority is check where cloud server is Authorize or not [5].CA is providing the certificate Authority. If any server is not recognizing with CA (Certificate Authority), then this server is Duplicate or Fraud server. Before uploading there data in the cloud, Data owner should check that Particular Server are Recognize with CA or not [6].

Logger- Cloud server is maintaining the logger. Logger is to be consisting of detail about user and the data owner who can Access the particular cloud server. Logger is playing the important role, while accessing cloud server of particular user. Also Logger should access the time and IP Address of data who user should requested [3].

Existing system- In the technique of cloud computing, it consist of Delivery to data from one resource to other machine through the internet. Now a day's one server should handle the Multiple Request of user. So that processing time will be increases simultaneously. So that the management of the database is not has trustworthy. Also web services are to be used for the Request and Response [4].

2.LITERATURE SURVEY

Cloud server:-Cloud server means user can use all types of data which is stored on the cloud server. Data owner can store his data on the cloud server. When user need data at that time user can send the request to the cloud server then cloud server accept the user request and pass to the data owner .when data owner accept the request of user then data owner search the data related to the user request then pass this data to the user throw the cloud server. The cloud server manages the information [1]



Certificate authority:We need the certificate authority in the cloud server for to confirm the cloud server again. When any cloud server is not responding then that server is called as fraud server. When data owner is stored on the cloud at that time he checks the cloud server means cloud server is confirming or not [2].

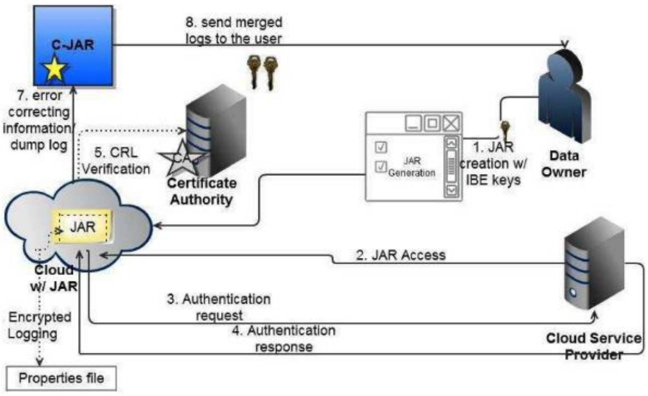
Jar availability:CIA contain log harmonizer to secure from attacks on offline JARs. Log harmonizer used to stores error correction information. It is also used to recover corrupted logs. It is also used to Decrypt the log records & handle duplicate records [5].

Logger:Cloud server is controlled to the logger. Loggers have all information of the data owner and users who are operating the Cloud Server. Logger will be used for user or data owner which operate the cloud server at specific time [3].

3.PROPOSED SYSTEM

We have proposed the new Method know as cloud Information Accountability. Totally Depends upon Information Accountability. Information Accountability is consists of secure transaction of data or file. In the information Accountability Without proper Authentication no one user should Access the particular server [1].One of the Advantage of the (CIA) Cloud Information Accountability is it has Ability to Maintain the low weight and powerful Accountability that Access the control or Authentication. Whole workings are to be done in the two Different modes known as: Push mode And Pull mode [3].

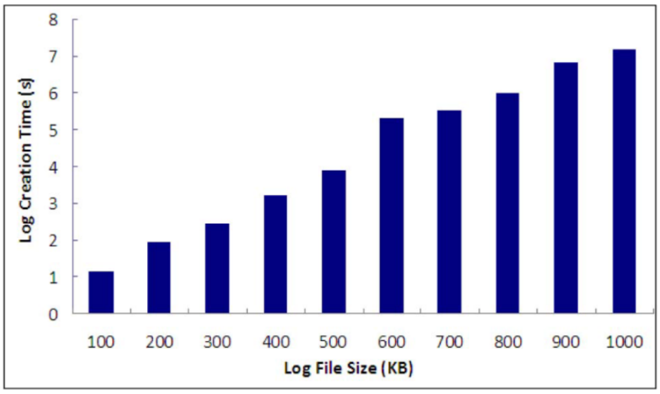
Detail Security Analysis Mechanism Are also provided.



```
1. Let TS (NTP) be the network time protocol timestamp.
2. Pull=0
3. Rec :=( UID, ode, Access Type, Result, Time, loc)
4. Cur Time: =TS (NTP)
5. Size=size of (log)//current size of the log
6. if ((cutime-tbeg) <time) &&
(Size < 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 ((cut time – beg) > time) || (size >=size) ||(pull!=0) then
16.//Check if PING is received
17. If PING-CJAR is received
18. PUSH log//write the log file to the harmonizer
19. RS (log): = NULL // reset the error correction records
20. Beg: = TS (NTP) //reset the beg variable
21. Pull: = 0
22. Else
23. Exit (1) // error if no PING is received
24. End if
25. End if
```

4.EXPECTED RESULT

Experimental result: In the experiment we first upon create the log file and measuring the total time overhead of the system. we can Analyze that in the whole experiment total time overhead is the ‘Authentication time’, ‘After encryption of log records’ and’ logs time combination’[7].our Architectural framework is light weight and the stored data are to be prove by Actual file and logs.



Authentication Time: During the Authentication of cusp, next point overhead should occur, but time duration of complete this authentication is so long [6].when any action required by JAR, the time taken for the authentication and user end is same.

Time Taken to Perform Logging: This is the main side of experiment .in which we have studies the effect of long file size or logging mechanism performance. We have also measured the average time, that should used to Access particular log record [4].the time for the execution is low due to the every access view the request. When action is about 10 sec then average time is so long or high.

5.CONCLUSION

We have introduced the new method or approach for the automatically logging mechanism. Logging mechanism is to provide the strong security of the server over the cloud. Also we have use the CIA which can help to support the Authentication mechanism. JARs file is the main aspect of the experiment. We have to increase the total speed of the file transmission in the low time over the cloud server.

REFERENCES

[1] *Cloud Computing, Principles and Paradigms* by John Wiley & Sons.

[2] *Ensuring Distributed Accountability for Data Sharing in the Cloud Author*, Smitha Sundareswaran, Anna

C.Squicciarini, Member, IEEE, and Dan Lin, *IEEE Transactions on Dependable and Secure Computing* VOL 9, NO,4 July/August 2012 .

[3] S. Pearson and A. Charlesworth, "*Accountability as a Way Forward for Privacy Protection in the Cloud*," Proc First Int'l conf. Cloud Computing, 2009.

[4]"*Reed-Solomon Codes and Their Applications*", S.B. Wicker and V.K. Bhargava, ed. John Wiley & Sons, 1999.

[5] Hsio Ying Lin,Tzeng.W.G, **"***A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding* ", IEEE transactions on parallel and Distributed systems, 2012.

6] Y. Chen et al., "*Oblivious Hashing: A Stealthy Software Integrity Verification Primitive*," Proc. Int'l Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.

[7] 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.