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. 2, Issue 12, December 2014

Highly Secure Public Data Verification Architecture Using Secure Public Verifier Auditor in Cloud Enviroment

Ritika Arora[1] Javed Akthar Khan [2]

Department of Computer Science &Engineering, RGPV University, Takshshila Institute of Engineering & Technology, Jabalpur, M.P India[1]

Department of Computer Science &Engineering, RGPV University, Takshshila Institute of Engineering & Technology, Jabalpur, M.P India[2]

ABSTRACT: As we all know the simple definition of Cloud computing means that the Service On Demand .The cloud computing and its work simple working concept is data stored in cloud for utilization .This data is used by cloud user at any time or in any place. In other word we can say that the cloud store the data these data is used by multiple user when they required .when data is store is in cloud server or cloud data center due to hardware failure , human failure and human mistake cloud data integrity is occur , the major problem is cloud computing is store a big amount of data in its server so it is not possible to retrieving entire file or data from the cloud server or solve this data integrity problem with proper high level security . so in this paper we are proposed a new cloud architecture for Third party auditor authentication with minimum auditing Time .

KEYWORDS: Cloud computing , Public Cloud ,Private Cloud , Hybrid Cloud ,Third party auditing **.**

I. Introduction

In the cloud storage Environment , users can remotely save their content and used software application already available in cloud server when they needed, user also able to shared his her data or information to other user cloud user use resources of cloud without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. This introductory section of cloud is some keyword of cloud computing .Nowadays cloud computing is a hot topic all over the world, through which customers can access information, software , resources without a arranging a basic requirement with the help of web browser or internet . Hence, it eliminates the need for maintaining expensive computing facilities. On the other hand a brief introduction about the cloud computing . A Cloud computing is an attractive and cost efficient continuation of server based computing [Ref -1] and application service provider model brief information about the cloud model explain Next Paragraph .We see cloud computing as a highly available computing environment where secure services and data are delivered on-demand pattern. There are so many definitions of Cloud computing .As per the National Institute of Standards and Technology (N IST) [Ref-2], says a cloud computing is "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. In this category we include Resources like Servers, Networks, Storage, and some Services that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Cloud [Ref-3] computing model are Public Cloud computing Model and Private Cloud Computing Model and Hybrid Cloud Computing Model .

10.15680/ijircce.2014.0212043

1.1 Public Cloud Computing

Public Cloud computing means relying on third parties to offer efficient IT services over the Internet as needed. Public Clouds are owned by the organization(s) selling Cloud services, The National Institute of Standards and Technology defines a public Cloud as a Cloud infrastructure that is made available to the general public or a large industry group

1.2 Private Cloud Computing

Private Cloud computing reassures the organization that their information and processes are more secure since everything is managed internally. According to the National Institute of Standards and Technology (NIST) a private Cloud is a Cloud infrastructure that is operated solely for an organization

1.3 Hybrid Cloud Computing Model

Hybrid Cloud computing is a combination of both private and public services

1.4 Cloud Computing Services

Infrastructure as a service (IaaS). Computing infrastructure, such as servers, storage, and network, delivered as a cloud service, typically through virtualization. Platform as a service (PaaS). Platforms that can be used to develop and deploy applications. Software as a service (SaaS). Software deployed as a hosted service and accessed over the Internet.

1.5 Public Verifier

Public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier.

1.6 Public auditing

Existing system allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing.

Data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking.

A public verifier could be a data user who would like to utilize the owner’s data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services

1.7 Privacy in public auditing

During public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud

1.8 Privacy to public verifiers

Sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. It is necessary to ensure the integrity of shared data in the cloud is correct. Existing public auditing mechanisms can actually be extended to verify shared data integrity.

This is Brief introduction of Cloud computing Environment , Rest of paper is organized as follows . In Section number Two , we briefly discuss related work Literature Review . Then we present the Problem definition in section number Three In section number Four we introduce a proposed new cloud architecture for Third party auditor authentication . In Section number five we are show the Audit graph and Performance Result . In Section number Six include a conclusion end of the paper show References used .

II. LITERATURE SURVEY

A careful analysis of literature on the variants and methodologies of privacy preserving in cloud computing reveals the following: So many method are already exiting for auditing cloud content before storing cloud Environment , this will be done Third person or some time called TPA .The user might give his/her identity of proof certificate [Ref-3] This paper includes the problems of misuse of the proof of identity (POI) certificate if fallen into unauthorized person. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal

10.15680/ijircce.2014.0212043

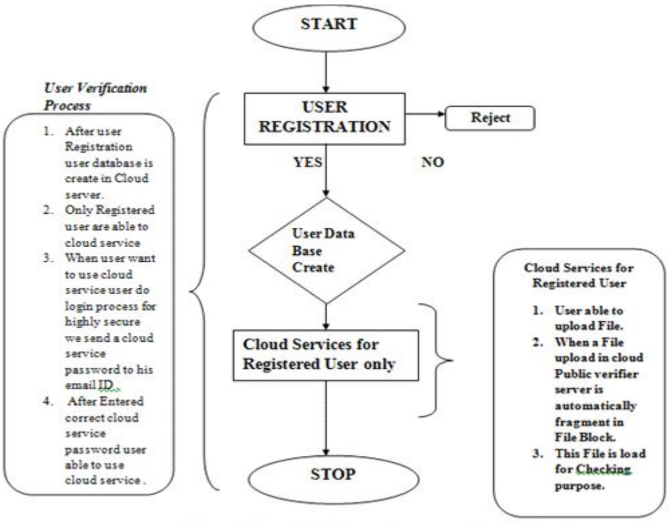
confidential information-identity privacy-to public verifiers. Bharathy S et al. decentralized key management work for providing a security to cloud data [Ref-4] Security and privacy protection in clouds are being explored by many researchers. Wang et al. [Ref- 6] addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptographic techniques has been studied in [Ref- 7]. Many homomorphic encryption techniques have been suggested [Ref- 8], [Ref- 9] to ensure that the cloud is not able to read the data while performing computations on them. HLA homorphic liner authenticaot [Ref-10] scheme is used by TPA to perform the auditing task in cloud , this work done in without demanding a local copy of data ,Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Drop box) or even personal information (as in social networking)

III. PROBLEM DEFINITION

After Reading a some paper mention in section two literature review integrity of data stored in the cloud can become compromised. To protect the integrity of data in the cloud and to offer “peace of mind” to users, it is best to introduce a third party public verifier/ auditor to perform auditing tasks on behalf of users but main problem is no body can ensure that third party auditor is secure . we are just assume third party auditor is trusted. There are so many task perform by third party public data verifier like computation/communication resources that users may not possess. Integrity of cloud data should be verified before any data utilization or share , such as search or computation over cloud data. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures or hash values of the entire data. Certainly, this conventional approach is able to successfully check the correctness of cloud data. The main drawback is new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers , apart from that a conventional architecture are not provide a data privacy , and no identity .

In we are show the simple working concept of Auditing task where data will be shared after completion auditing task , this task is done by public verifier / auditor. So during literature survey I am read so many method describe for solving this problem . data will be audit by public verifier now here we just assume that a public verifier is doing his work honestly , solving this problem I have introduce a new cloud data public verifier architecture that supervise a working of third part public auditor .

IV. PROPOSED ARCHITECTURE



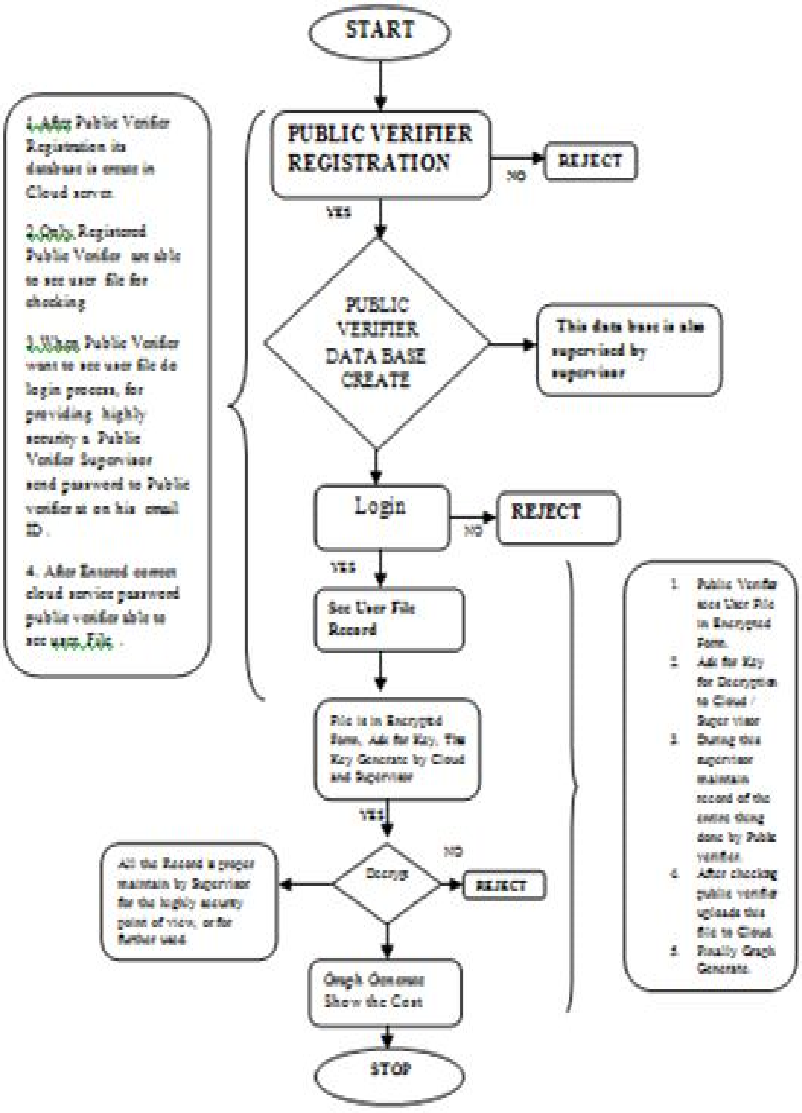
User Verification Process

1. After user Registration user database is create in Cloud server.
2. Only Registered user are able to cloud service
3. When user want to use cloud service user do login process for highly secure we send a cloud service password to his email ID.
4. After Entered correct cloud service password user able to use cloud service .

Cloud Services for Registered User

1. User able to upload File.
2. When a File upload in cloud Public verifier server is automatically fragment in File Block.
3. This File is load for Checking purpose.

User Registration Process Architecture


START
PUBLIC VERIFIER REGISTRATION
NO
REJECT
YES
PUBLIC VERIFIER DATA BASE CREATE
This data base is also supervised by supervisor
1.After Public Verifier Registration its database is create in Cloud server.
2.Only Registered Public Verifier are able to see user file for checking
3.When Public Verifier want to see user file do login process, for providing highly security a Public Verifier Supervisor send password to Public verifier at on his email ID .
4. After Entered correct cloud service password public verifier able to see user File .
Login
NO
REJECT
YES
See User File Record
File is in Encrypted Form, Ask for Key, The Key Generate by Cloud and Supervisor
YES
Decrypt
NO
REJECT
All the Record a proper maintain by Supervisor for the highly security point of view, or for further used.
Graph Generate Show the Cost
STOP
1. Public Verifier sees User File in Encrypted Form.
2. Ask for Key for Decryption to Cloud / Super visor
3. During this supervisor maintain record of the entire thing done by Public verifier.
4. After checking public verifier uploads this file to Cloud.
5. Finally Graph Generate.

Public Verifier Registration Process Architecture

V. RESULT

Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity and we show the improve result via auditing graph shown in this paper

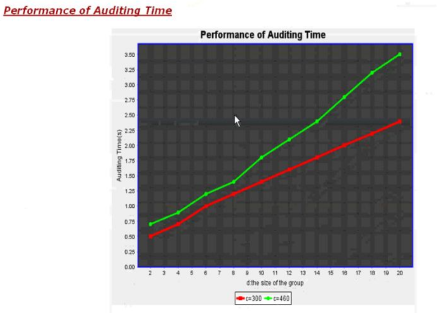


Figure Performance OF Auditing Time Graph

Graph is Generated during complication of all work of User and Public verifier .

VI. CONCLUSION

We have used the new architecture for providing a high security with proper manage of Third party auditor database in cloud this record will be mange by Public auditor Supervisor . this all the record is very help full for further utilization if any deficiency is occur , one more thing all the Third party working is supervised by public auditor supervisor this is provide a more security . we also make a improved graph for all work done by public verifier .

REFERENCES

1. 91-US-31-1_Cloud_Computing White Paper Cloud Computing: Thin clients in the clouds. (2009)
2. The NIST Definition of Cloud Computing. Retrieved March 15, 2012 from http://www.nist.gov/itl/cloud/upload/cloud def-v15.pdf
3. Buecker. A., Lodewijkx. K., Moss.H., Skapinetz. K., & Waidner. M. (2009).Cloud Security Guidance. IBM Recommendations for the Implementation of Cloud Security. Cloud security: the grand challenge. Retrieved April 16, 2012 from http://www.redbooks.ibm.com/redpapers/pd fs/redp4614.pdf
4. Bertino, E.; Paci, F.; Ferrini, R.2009 Privacy-preserving Digital Identity Management for Cloud Computing, IEEE Computer Society Technical Committee on Data Engineering.
5. Divya bharathy S, Ramesh T 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14) On 21st& 22nd March Organized by K.L.N. College of Engineering, Madurai, Tamil Nadu, India International Journal of Innovative Research International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014ISSN (Online) : 2319 – 8753 ISSN (Print) :2347 – 6710
6. C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.
7. H. Li, Y. Dai, L. Tian, and H. Yang,"Identity-based authentication for cloud computing," in *Cloud Com*, ser. Lecture Notes in Computer Science, vol. 5931.Springer, pp. 157–166, 2009.
8. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. Dissertation, Stanford University, 2009 http://www.crypto.stanford.edu/craig.
9. A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token -based cloud computing," in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer,pp. 417–429, 2010.
10. Privacy-Preserving Public Auditing for Secure Cloud Storage IEEE 2013 Transaction, Computers,Â Feb 2013
11. Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds Sushmita Ruj‡,
12. H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures:Achieving attribute-privacy and collusion resistance,"*IACR Cryptology e Print Archive, 2008.*
13. F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011 [Ref-14] Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", IACR Cryptology ePrint Archive, 419, 2012
14. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *IEEE TrustCom*, 2011.