ISSN: 2320-1363

Enhancing Availability Using Identity Privacy Preserving Mechanism in Cloud Data Storage

V.Anjani Kranthi [*1], Smt.D.Hemalatha [*2]

M.Tech Student, Dept of CSE, S.R.K.R engineering college, Bhimavaram, AP, India,

Assistant Professor, Dept of CSE, S.R.K.R engineering college, Bhimavaram, AP, India,

ABSTRACT:

Cloud computing is the backbone to the technology driving. Cloud computing technology provides services like access files and shared files. Data integrity is the major issue. Different mechanisms have been designed previously to support public auditing on shared data store in the cloud. Many public verifiers are available to verify under shared data for integrity. Cloud users were not received any integrity and data freshness results. Finally traceability recognized as an issue.

This paper is designed with traceability mechanism. It can improve data privacy and achieving traceability and data freshness using identity privacy mechanism. Compare to previous approach, enhanced approach improves availability and integrity.

INDEX TERMS: cloud data storage, privacy preserving mechanism, availability, identity privacy, public verifier.

I.INTRODUCTION

Cloud computing is the computing of the large number of connected devices in terms of data storage and online access. The most important privacy related to security and how cloud provides its service assurance are major issues. Currently many third party service providers and security models ensure to handle security issues. These are not fit and efficient frameworks.

Data protection is required in transit and in remaining environments it is good service. To solve the privacy issue on shared data new identity privacy mechanism has been proposed here. It improves data privacy on shared data. Using proposed concepts we achieve traceability, data freshness. Through data freshness feature users gets latest version of files information. Here rollback attackers and mis-configuration errors are reduced here.

ISSN: 2320-1363

II.RELATED WORK:

Today all networking users are accessing cloud services from different remote locations. Private cloud data storage always needs to maintain data privacy and integrity for users. Cloud is ready to provide different categories of services. Under service distribution we can observe some kind of privacy issues. Privacy preserving mechanism allows public auditing of shared data stored in the cloud. Many of existing approaches are implemented for privacy purpose under storing and share data environment.

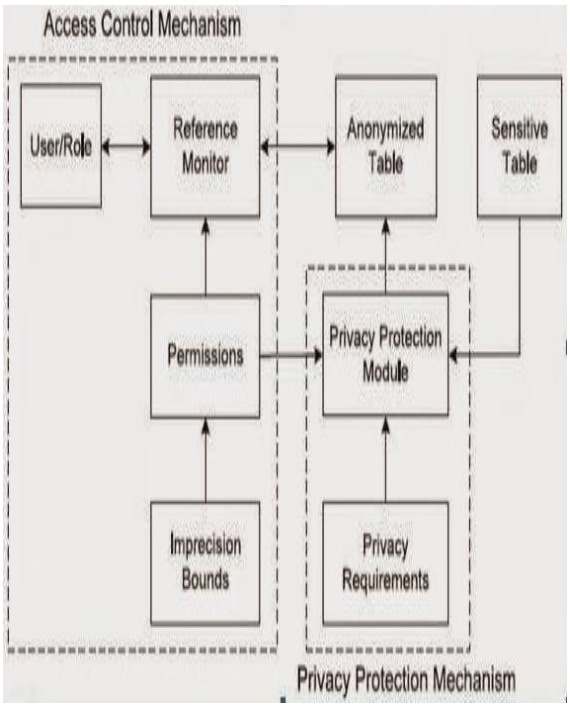

Fig1: Privacy Preserving Mechanism

Privacy preserving auditing technique can work on group of users. Privacy preserving auditing techniques design with homomorphic authentication mechanism. Homomorphic authentication mechanism uses pseudo random function and group signature also. These techniques verifies each and every block. It reduces the space to store the verification data. After designing these techniques privacy issues are available in cloud. These are designed with five algorithms.

1. Key generation
2. Join algorithm
3. Sign
4. Proof generation
5. Proof verification

Authenticated File System is also a privacy preserving mechanism. It is completely related to oruta. AFS have lack of data freshness functionality. It works on data file operations. Here two layers are available for data freshness. Lower layer store blocks, each and every block will have MAC and version number information. Upper layer consist of Markel tree information. Every block versions are update here based on time interval. Again some issues we can observe here in this current auditing mechanism.

Another privacy preserving mechanism we can introduce here that is called homomorphic authenticator with random

ISSN: 2320-1363

masking. Random masking operation can perform on each and every block using pseudo random function. Here different steps are involved. Those steps are

1.setup

2. Audit

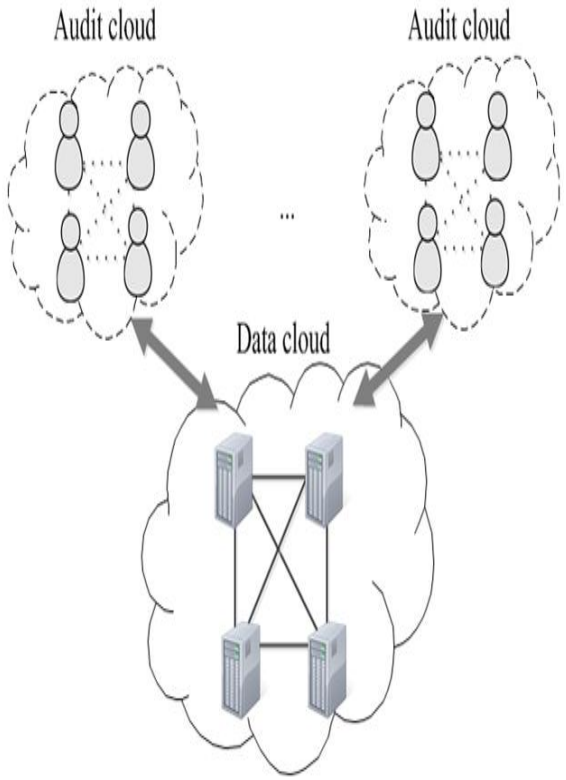

Fig2: Public auditing mechanism diagram

Setup: generate signature for each and every block.

Audit: we can except challenge message from third party auditor.

This approach does not work efficiently up to the mark.

Finally last existing third party procedure is called ORUTA. It does not reveal any identity of the user. Here many problems we observed like forge ability and less verifiability problems. All existing approaches issues can control in this paper.

II.PROBLEM STATEMENT

Data integrity is one of the major issue. This is lack of identity privacy. Public verifier audits shared data and checks integrity of shared data. Enhance the model in order to audit the data integrity and keeping identity privacy also. We can achieve different number of constraints related to privacy and security.

1. Correctness

2. Availability

3. Public auditing

III.PROPOSED METHODOLOGY

Here we are going to design traceability framework for achieving availability. Traceability is classifying into two categories of users.

1. Fake users

2. Normal users

ISSN: 2320-1363

Fig3: identity management Security

Data owner store the data in cloud. Cloud owner gives public key to data owner and cloud user or group members. Combine of public key and private key it is possible to generate group signature. Group signature is distributed to all cloud private users. During auditing Public verifier verifies private key and public key and identity of the signer also. Any key is leaked then we have different characteristics here for detection. Those are

1. Traceability
2. Public auditing
3. Correctness
4. Identity privacy
5. Data freshness

Traceability: tracking fake user from accessing the data from cloud.

Public Auditing: public verifier checks the integrity of shared data.

Correctness: public verifier verifies the correctness of shared data integrity.

Identity Privacy: verify whether the user is fake user or normal user.

Data Freshness: Protect against mis-configuration errors.

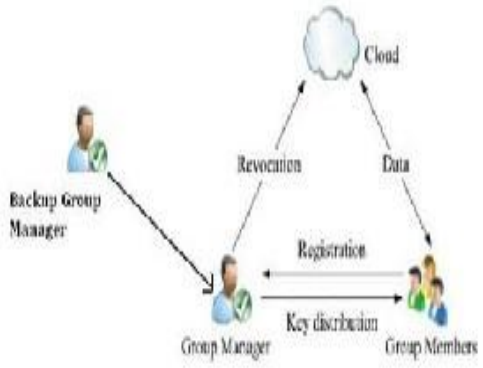

Fig4: Identity key distribution

System model consist of three types of users. Those are cloud owner, data owner, cloud user or group of users. Different types of users are participated here.

1. Original user
2. Group of users

Every member have permission to access and allow modify and shared data. After shared data operation we can perform

ISSN: 2320-1363

verification with signature. Signature verification gives report whether it is integrity or not.

IV.EXPERIMENTAL RESULTS AND DISCUSSION

Different trusted third party auditors learn unauthorized information through auditing mechanism. We can observe practical results of Existing and proposed approaches through authorization and authentication of shared data in cloud data storage.

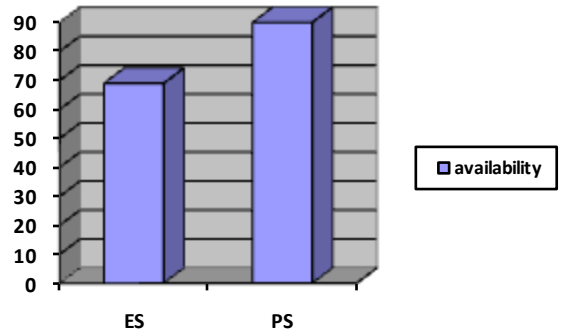

Fig5: Performance Graph

Graph explains about existing and proposed system availability results. Proposed system gives high availability results compare to existing system.

V.CONCLUSION AND FUTURE WORK

In this paper we designed identity privacy mechanism for shared data in the cloud. This new mechanism is adopted to achieve traceability and data privacy. Public verifier verifies shared data and achieves new updated data collection. It detects more number of fake users and enhanced cloud data storage availability.

We observe many difficulties in current system; all those are control with future auditing system.

VI.REFERENCES

[1] Boyang Wang, Baochun Li, Hui Li, Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud in IEEE transactions on cloud computing, VOL. 2, NO. 1, 2014, page no:43-56.

[2] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[5] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

ISSN: 2320-1363

[7] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.
[8] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.
[9] The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/html/rfc1321, 2014.
[10] G. Attendees, R. Burns, R. Carmela, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.
[11] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90- 107, 2008.