Privacy Preservation using Shamir's Secrete Sharing Algorithm for Data Storage Security

Tejashree Paigude[#], Prof. T. A. Chavan[*]

[#]*P.G Scholar, Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune University Pune-41, India*

[*]*Assistant Professor, Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune University Pune-41, India*

ABSTRACT: *The Cloud computing is a latest technology which provides various services through internet. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this paper, we proposed a Shamir's Secrete sharing algorithm for Privacy Preservation for data Storage security in cloud computing. We can achieve confidentiality, integrity and availability of the data. It supports data dynamics where the user can perform various operations on data like insert, update and delete as well as batch auditing where multiple user requests for storage correctness will be handled simultaneously which reduce communication and computing cost.*

Keywords—*Privacy Preserving, Public Auditing, TPA, Data Security*

1. INTRODUCTION

Cloud Computing is using hardware and software as computing resources to provide service through internet. Cloud computing provides various service models as platform as a service (PaaS), software as a service (SaaS), Infrastructure as a service (Iaas), storage as a service (STaaS), security as a service (SECaaS), Data as a service (DaaS) & many more. Out of this Paas, SaaS and IaaS are most popular.

Cloud computing has four models as Public cloud: though which the service is available to all public use. Private cloud: Through which service is available to private enterprise or organization. Community Cloud: It allows us to share infrastructure among various organizations through which we can achieve security. We can achieve security by internal members or else by external Third party vendor. Hybrid cloud: it is a combination of public and private cloud. Cloud computing has many advantages as: we can easily upload and download the data stored in the cloud without worrying about security. We can access the data from anywhere, any time on demand. Cost is low or pay per usage basis. Hardware and software resources are easily available without location independent. The major disadvantages of cloud computing is security.

2. LITERATURE SURVEY

2.1 Security Issues

The security is a major issue in cloud computing. It is a sub domain of computer security, network security or else data security. The cloud computing security refers to a broad set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud computing. Some security and privacy issues that need to be considered are as follows

1) *Authentication:* Only authorized user can access data in the cloud
2) *Correctness of data:* This is the way through which user will get the confirmation that the data stored in the cloud is secure
3) *Availability:* The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data
4) *No storage Overhead and easy maintenance***:** User doesn't have to worry about the storage requirement & maintenance of the data on a cloud
5) *No data Leakage:* The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.
6) *No Data Loss:* Provider may hide data loss on a cloud for the user to maintain their reputation.

In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider or cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud without worrying about storage and maintenance. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of

data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done.

Security in cloud computing can be addressed in many ways as authentication, integrity, confidentiality. Data integrity or data correctness is another security issue that needs to be considered. The proposed scheme [4] specifies that the data storage correctness can be achieved by using SMDS (Secure Model for cloud Data Storage). It specifies that the data storage correctness can be achieved in 2 ways as 1) without trusted third party 2) with trusted third party based on who does the verification.

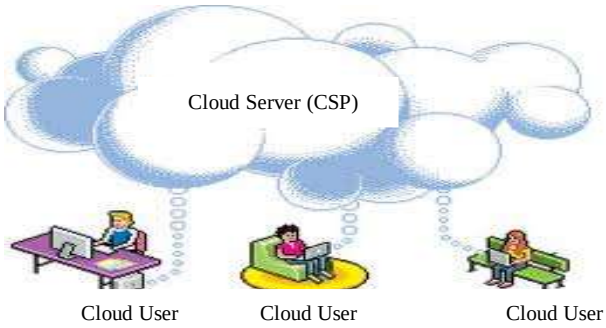

Fig 1: Cloud Architecture

It provides data confidentiality in two stages as 1) Data at rest 2) Data in transmission.

1) Data at rest: Symmetric key encryption technique (i.e. AES, TDES, and DES) are recommended which are secure but more time consuming.

2) Data in transmission: Secure Socket Layer (SSL) protocol is used for integrity verification. It uses a two different hash function such as Secure Hash Algorithm (SHA1) for digital signature and Message Digest (MD5) is a cryptographic hash function which is used to check the data integrity.

Balkrishna and Hoka address problem of access control using cryptographic techniques which degrades performance and increase the computation cost of managing all keys at Cloud Server and at the user[13][22]. They proposed Diffie Hellman key exchange scheme for sharing symmetric key securely. Researchers of [4] specify way to achieve storage correctness without Trusted Third Party (TTP). Following are major goals of proposed schemes as

- CS neither should learn any information from user's data nor should misuse the same.
- The User selects the encryption option for their data
- Secure key management
- Flexible access right managements
- It aims to achieve light weight integrity verification process for checking the unauthorized change in the original data without requesting a local copy of the data.

It uses public key encryption technique to encrypt the data for data storage correctness. It achieves the following goals as data confidentiality, security, light weight verification, key management, access right and no data duplication.

The proposed scheme is compared with different cloud service providers like cloudseal, cloud zone, Venus & EPPS. It uses symmetric encryption which provides confidentiality, integrity, and verification With low cost. It also provides authentication for data owner and access control through which only authorized user can access the data.

The correctness of data can be violated due to internal and external threats and CSP may hide data loss or damage from users to maintain a reputation. Major security issues associated with cloud user and CSP are as follows

1) Cloud Service Provider (CSP): Organization or enterprises provide various services to cloud users. Confidentiality and integrity of cloud data should be maintained by CSP. The Provider should ensure that user's data and application are secured on a cloud. CSP may not leak the information or else cannot modify or access user's content. The attacker can log into network communication [9].

2) Cloud Server (CS): The cloud server where data being stored and accessed by cloud data owner or users. Data should not be accessed by unauthorized users, no data modification or no loss of data.

3) *Cloud User:* Attackers can access basic information like username and password [9]. Key management is major issue in encryption techniques. Data dynamic issues need to be considered by CSP.

Cloud Computing Threads [9] are as follows:

- Spoofing Identity Theft
- Data Tempering Threat
- Repudiation Attack
- Information Disclosure on up/download Intra-Cloud
- Denial of Service Attack
- Log In

To achieve security, we can handover our data to a third outsource party who will specify the correctness and integrity of the cloud data. Hence, new concept arrives as Third party auditor (TPA) who will audit the user data stored on the cloud, based on the user's request. In this case, the Cloud service provider doesn't have to worry about the correctness and integrity of the data. In this technique, TPA will audit the cloud data to check the integrity or correctness in two ways as: 1) Download all files and data from the cloud for auditing. This may include I/O and network transmission cost. 2) Apply auditing process only for accessing the data but again in this case, data loss or data damage cannot be defined for unaccessed data. Public auditability allows user to check integrity of outsource data under different system & security models. We cannot achieve privacy as TPA can see the actual content stored on a cloud during the auditing phase. TPA itself may leak the information stored in the cloud which violate data security. To avoid this, Encryption technique is used where data is encrypted before storing it on the cloud.

Through this, they achieved privacy up to certain extent but which increases complex key management on user side. This technique cannot be long lasting as unauthorized user can easily access original content by using the decryption key which is easily available. Hence to achieve privacy preservation with public auditing using TPA for cloud data storage security, researchers have proposed various techniques.

3. EXISTING SYSTEM

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server / cloud service provider (CSP). Cloud user stores large amount of data or files on a cloud server. User can upload their data on cloud server (CS) and that data will be managed by cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data.

The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, Third Party Auditor allows checking the integrity of data. It supports privacy preservation

In cloud, data is stored in a centralized form and managing this data and providing security is very difficult. During auditing phase, TPA can read the user's data hence can modify. The reliability is increased as data is handled by TPA but data integrity is not achieved. It uses encryption technique to encrypt the contents of the file.

TPA checks the integrity of the data stored on a cloud but if the TPA itself leaks the user's data. Hence the new concept comes as auditing with zero knowledge privacy where TPA will audit the users' data without seeing the contents. It uses public key based homomorphic linear authentication (HLA) [1], [2] which allows TPA to perform auditing without requesting for user data. It reduces communication & computation overhead. In this, HLA with random masking protocol is used which does not allow TPA to learn data content.

3.1 Goals

- It allows TPA to audit users' data without knowing data content
- It supports batch auditing where multiple user requests for data auditing will be handled simultaneously.
- It provides security and increases performance through this system.

3.2 Design Goals

1) *Public audit ability:* Allows third party auditor to check data correctness without accessing local data.
2) *Storage Correctness:* The data stored on a cloud is as it. No data modification is done.
3) *Privacy preserving:* TPA can't read the users' data during the auditing phase.
4) *Batch Auditing:* Multiple users auditing request is handled simultaneously.
5) *Light Weight:* Less communication and computation overhead during the auditing phase.

and for integrity check user as well as third party auditor can check the integrity of the data where we can achieve publicly auditing user data. It supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance.

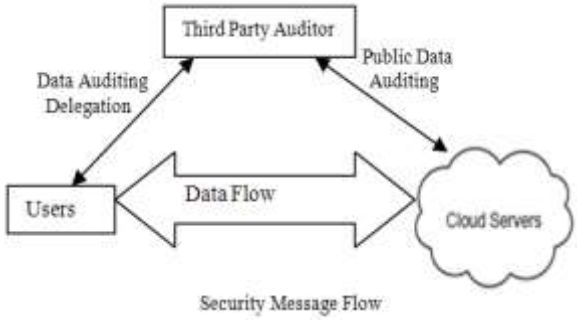

Fig 3: Architecture of Data Security in Cloud Using TPA

4. PROPOSED SCHEME

The data on the cloud has a minimum concern about sensitive information such as social security number, medical records, bank transaction and shipping manifests for hazardous material. We provide additional security by using Shamir's secret sharing algorithm. Shamir's Secret Sharing is an algorithm in cryptography. It is developed by Adi Shamir. Secret data is divided into multiple parts or shares, which will be stored at multiple different clouds. To reconstruct the original data from multiple shares, we need to have at least k or more shares. WE cannot reconstruct the original data with share value than (k-1).

We don't need all shares to reconstruct the original data and therefore the threshold value (k) is used where any k of the parts are sufficient to reconstruct the original secret.

4.1 Design Goals

The goal is to divide data D (e.g., a safe combination) into n pieces D1,….,Dn in such a way that:

1. Knowledge of any k or more Di pieces makes D easily computable.
2. Knowledge of any k-1 or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (k,n) threshold scheme. If k=n then all shares are required to reconstruct the original data.

Advantages of Proposed scheme

1. Secure: Information theoretic security.
2. Minimal: The size of each piece does not exceed the size of the original data.
3. Extensible: When k is kept fixed, we can add or delete Di shares dynamically without affecting other.

4. Dynamic: We can change the polynomial to increase the security and we can reconstruct the new shares.
5. Flexible: for authentication, we can maintent the security unlock categories based on its hierarchy.

4.2 Mathematical Model

Suppose we want to use a (k, n) threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size 0<k<=n<P where P a prime number.

Choose at random k-1 coefficients a1 ...ak-1 in F, and leta0=S. Build the polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$$

Let us construct any n points out of it, for instance set $i = 1, \cdots, n$ to retrieve $(i, f(i))$ .Every participant is given a point (a pair of input to the polynomial and output).with k shares, we can find the coefficients of the polynomial using interpolation and the secret is the constant term a0.

4.2.1 Preparation

Suppose that our secret is 1234 (S=1234). We wish to divide the secret into 6 parts (n=6), where any subset of 3 parts (k=3) is sufficient to reconstruct the secret. At random we obtain two (k-1) numbers: 166 and 94. (a1=166; a2=94)

Our polynomial to produce secret shares (points) is therefore:

$$F(x) = 1234 + a66x + 94x^2$$

From the above polynomial, we construct following six points: (1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614) On each cloud will store this shares separately as (x and f(x)).

4.2.2 Reconstruction

The value of k=3, so we need to have atleast three shares to reconstruct the original data. Let us consider

$$(x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414).$$

To reconstruct the original data, we use Lagrange basis polynomials:

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$
$$= 1234 + 166x + 94x^2$$

Recall that the secret is the free coefficient, which means that S=1234, and we are done.

4.3 Proposed System Workflow

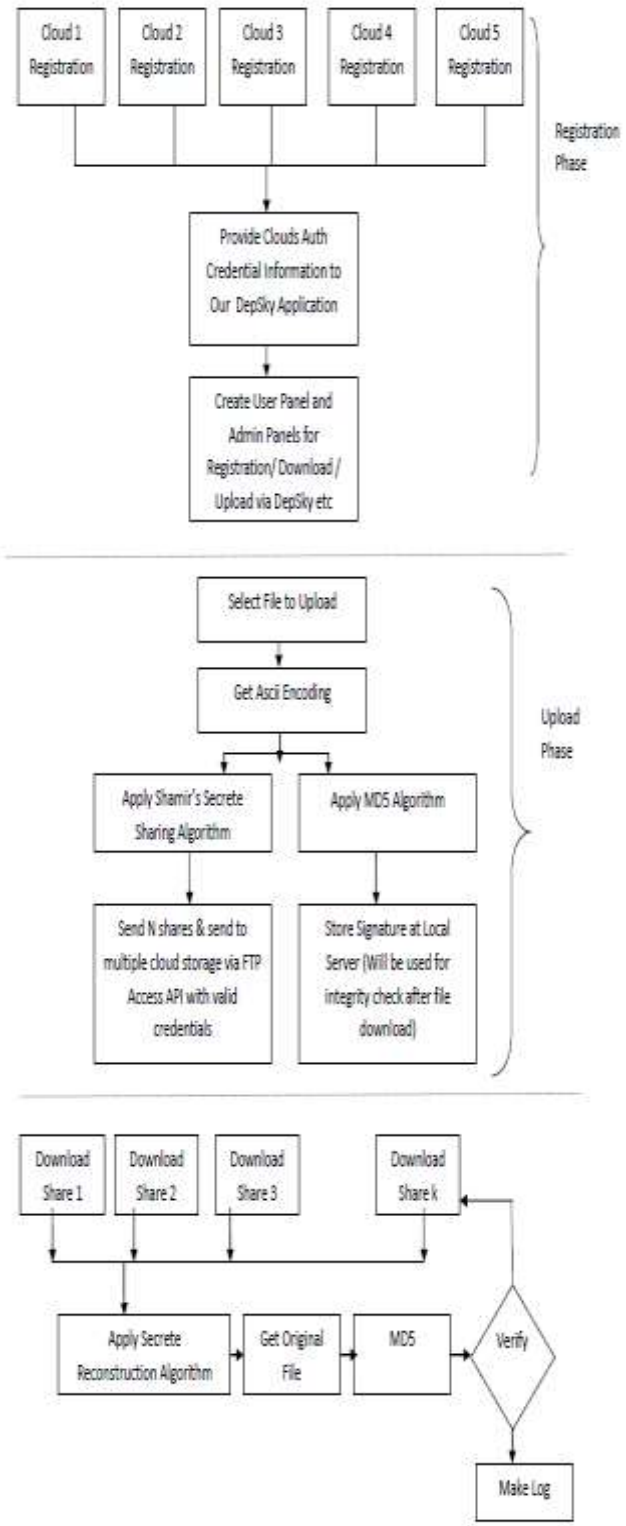

Fig 4.1 System Workflow

4.4 Screen Shots

Fig 4.2 File Upload

Fig 4.3 File Download

4.5 Result and Discussion

One can draw an infinite number of polynomials of degree 2 through 2 points. Unique polynomial of degree 2 can be defined with three points. This image gives better explanation for shamir's algorithm which is based on polynomial of finite field. That can't be represented in 2D plane

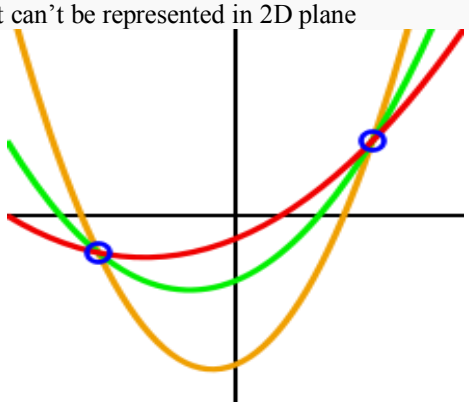

Fig 4: Analysis proof of Shamir's Secrete Sharing

This scheme specifies that 2 points required drawing line, 3 points for parabola and 4 points for cubic curve and so on. Similarly we need k points to define polynomial of degree k-1

5. CONCLUSIONS

In this system, we proposed Shamir's Secrete sharing algorithm for Privacy Preservation with Public Auditing for cloud data storage security. Cloud computing security is a major issue that needs to be considered**.** Using TPA, We can verify the correctness and integrity of data stored on a cloud. It uses Shamir's Secrete Sharing algorithm along with public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preservation data security. We achieved zero knowledge privacy through random masking technique. The proposed algorithm is very efficient and strong algorithm through which we have achieved confidentiality, integrity and availability of cloud data.

REFERENCES

[1] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, *"*Privacy-Preserving Public Auditing for Secure Cloud Storage*",IEEETrasaction on Computers I,* vol. 62, no. 2, pp.362-375 , February 2013.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, *"*Privacy-Preserving Public auditing for storage security in cloud computing*", in Proc.of IEEE INFOCOM'10, March 2010.*

[3] Wang Shao-hu, Chen Dan-we, Wang Zhi-weiP, Chang Su-qin, *"*Public auditing for ensuring cloud data storage security with zero knowledge Privacy*" College of Computer, Nanjing University of Posts and Telecommunications, China, 2009*

[4] KunalSuthar, Parmalik Kumar, Hitesh Gupta, *"*SMDS: secure Model for Cloud Data Storage*", International Journal of Computer applications, vol56, No.3, October 2012*

[5] AbhishekMohta, Lalit Kumar Awasti, *"*Cloud Data Security while using Third Party Auditor*", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, ISSN 2229-8 June 2012.*

[6] Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li *"*Enabling Public Audatability and Data Dynamics for Storage Security in Cloud Computing*", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 – 859,2011.*

[7] D. Shrinivas, *"*Privacy-Preserving Public Auditing in Cloud Storage security*", International Journal of computer science and Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011*

[8] K Govinda, V. Gurunath prasad and H. sathish kumar, *"* Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA*", International Journal of Advanced science and Technical Research, vol 4,no. 2, ISSN: 2249-9954,4 August 2012*

[9] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, *"*Implementation of EAP with RSA for Enhancing The Security of Cloud Computig*", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012*

[10] XU Chun-xiang, HE Xiao-hu, Daniel Abraha, *"*Cryptanalysis of Auditing protocol proposed by Wang et al. for data storage security in cloud computing", *http://eprint.iacr.org/2012/115.pdf, and cryptology eprint archive: Listing for 2012.*

[11] B. Dhiyanesh"A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" , *International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 6602 3127, 2011*

[12] C. Wang, Q. Wang and K. Ren, *"*Ensuring Data Storage security in Cloud Computing*",IEEE Conference Publication, 17th International Workshop on Quality of Service (IWQoS), 2009*

[13] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan. S, *"*Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud*", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012*

[14] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, *"*Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing*", International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012*

[15] LingarajDhabale, PritiPavale, *"*Providing Secured Data Storage by Privacy and Third Party Auditing In Cloud*", International Conference on Computing and Control Engineering, ISBN 978-1-2248-9, 12 & 13 April, 2012*

[16] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. *,"*Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing*",Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012*

[17] Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A. Deshmukh, *"*Investigation of TPA (Third Party Auditor Role) foe Cloud Data Security*", International Journal of Scientific and Engineering Research, vo. 4,no. 2,ISSn 2229-5518, Feb 2013.*

[18] Gayatri. R, *"*Privacy Preserving Third Party Auditing for Dynamic Data*", International Journal of Communication and engineering, vol. 1, no. 1, issue: 03, March 2012*

[19] Prince Jain "Security Issues and their solution in cloud computing", *International Journal of computing and business research, ISSN (Online): 2229-6166*

[20] Amala "Dynamic Audit Services for Achieving Data Integrity in Clouds", *International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021*

[21] R.Ushadevi V. Rajamani, "A Modified Trusted Cloud Computing Architecture based on Third Party Auditor (TPA) Private Key Mechanism", *International Journal of Computer Applications (0975 – 8887) Volume 58– No.22, November 2012*