A SURVEY ON SECURE THIRD PARTY AUDITING OF USERS IN CLOUD COMPUTING

[1]Nikita .D. Chandure , [2]Prof.Sachin .A. Murab, [3]Prof.Aniruddha.A.Kolpyakwar
[1]Student M.E 2nd Year, [2]H.O.D, [3]Assistant Professor
[1,2,3] Department Of Computer Engineering ,
[1,2,3] Jagadambha College of Engineering & Technology, Yavatmal , India.

Abstract : Now a days the use of the cloud computing is on the peak where it is at public, personal level. The cloud service providers (CSP) provide the cloud server to the its end users. To regulate the working of cloud service providers in a fair way the concept of the data audit is emerged for its user. The company which does the data audit is called as third party auditor(TPA). The third party has some rights while it can misused the data while auditing by selling it to third party. TPA audits to check the data integrity. TPA can data audit of a user or a group of users. To maintain the data privacy of data of data owner we are going to use along with the user signature is document signature i.e the signature on each data content of user. In this we are going to solve this problem by performing various auto signature generation techniques over each and every file upload or share document by user with privacy preserving over cloud.

IndexTerms - CSP, TPA, data audit, signature, data integrity, etc

I. INTRODUCTION

Cloud computing is a type of internet based computing that provides shared computer processing resources and data to computers and other devices on demand, and provide the storage space to the users to store their documents, images, songs etc, can also retrieve whenever they want.

Cloud Service Providers (CSP) provide the services to the users and also manage an enterprise infrastructure class that offers a scalable, reliable and secure environment to the users, and requires a very low marginal cost to the sharing nature of resources

Cloud model is composed of three service models. First, Software as a Service (SaaS) provides the capability to its users, to run their applications on cloud infrastructure. Second, Platform as a Service (PaaS) provides a platform to users to perform operations like develop, run, and manage applications. Third, Infrastructure as a service (IaaS) provides virtualized hardware support to its users so that they can save their investments over expensive local hardware requirements.

Data Owner may be worried about various security issues like the data might be accessed or altered in illegal way. In this paper we are focusing to maintain the integrity of outsourced data through auditing of that data. There is basically two categories of Auditing schemes, Private Auditing and Public Auditing. Private auditing is an initial auditing model for checking integrity of outsourced data, In private Auditing scheme all computation that need for checking integrity is directly performed between data owner and cloud service provider. This scheme has its own advantage and disadvantage, its main advantage is that, it can preserve privacy of data but the overload that increase on Data Owner side is not good at all and also it can happen that data owner and CSP both do not trust on each other about integrity proof results. Second type of Auditing is Public Auditing, in which integrity verification process is done by TPA (Third Party Auditor). This scheme reduces the computation overhead of user because all computations are done through Third Party Auditor and integrity verification results produced by third party auditor are commonly accepted by both data owner and CSP.

Cloud computing has four types of deployment models. First, Private cloud delivers its services same as public cloud but dedicate to single user or organization. Second, Public cloud provides its services shared over multiple users and organizations. Third, Hybrid cloud is a combination of Public cloud and Private cloud as it works like Private cloud but can access more computing resources from third party to enhance its performance. Fourth is Community cloud, as its name suggests that its services are shared over multiple organizations. As we know three main pillars of security is CIA (Confidentiality, integrity, availability) belonging to same working area or we can say community.

II. LITERATURE REVIEW

The first provable data possession (PDP) mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without retrieving the entire data. Moving a step forward, (referred to as WWRL) is designed to construct a public auditing mechanism for cloud data, so that during public auditing, the content of private data belonging to a personal user is not disclosed to the third party auditor [7].

Construct an aggregate signature scheme based on a recent short signature due to Boneh, Lynn, and Shacham (BLS) [19].
Recent visions of "cloud computing" and software as a service call for data, both personal and business, to be stored by third parties, but deployment has lagged [16].

Existing work introduced a dynamic audit service for integrity verification of untrusted and outsourced storages. Audit system can support dynamic data operations and timely anomaly detection with the help of several effective techniques, such as fragment structure, random sampling, and index-hash table (IHT) [8].

Specifically, the data owner encrypts blocks of content with symmetric content keys. The content keys are all encrypted with a master public key, which can only be decrypted by the master private key kept by the data owner. The data owner uses his master private key and user's public key to generate proxy re-encryption keys [20].

Digital signatures are the most important cryptographic primitive for the daily life. Short signature is a variant of digital signature which can provide a high security level with relatively shorter signature length [5].

Homomorphic signature schemes have been initially designed to establish authentication in network coding and to address pollution attacks. However, since they allow for computations on authenticated data, they are also a useful primitive for many other applications [21].

Homomorphic authenticators (also called homomorphic verifiable tags) are basic tools to construct data auditing mechanisms. Besides unforgeability (only a user with a private key can generate valid signatures), a homomorphic authenticable signature scheme, which denotes a homomorphic authenticator based on signatures [7].

A ring signature scheme allows a signer to sign a message on behalf of a set of users which include the signer herself in such a way that a verifier is convinced that the signer is one of the ring members, but he cannot tell which member is the actual signer [14].

A ring signature scheme is set-up free: The signer does not need the knowledge, consent, or assistance of the other ring members to put them in the ring - all he needs is knowledge of their regular public keys. Different members can use different independent public key signature schemes, with different key and signature sizes. Verification must satisfy the usual soundness and completeness conditions, but in addition we want the signatures to be signer-ambiguous in the sense that the verifier should be unable to determine the identity of the actual signer in a ring of size r with probability greater than 1/r [22].

Common to the existing techniques is the fact that they employ a trusted server that stores the data in clear. Access control relies on software checks to ensure that a user can access a piece of data only if he is authorized to do so [23].

Consider public auditability in their "Provable Data Possession" (PDP) model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphic linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file. However, among their two proposed schemes, the one with public auditability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor [9].

As part of pre-processing, the client may alter the file to be stored at the server. The client may expand the file or include additional metadata to be stored at the server. Before deleting its local copy of the file, the client may execute a data possession challenge to make sure the server has successfully stored the file Clients may encrypt a file prior to out-sourcing the storage. [16].

Yanru Zhang, Xiang-Yang Li, and Zhu Han proposed the idea of utilizing punishment to diminish CSP's motivation to cheat from an agreement hypothetical viewpoint, where cloud benefit clients can depend on an outside evaluator to check the calculation comes about when required.

J.Raja, Dr. M.Ramakrishnan proposed security protection of information utilizing TPA administrations. It uses people in general key examining and arbitrary concealing techniques that guarantee that TPA couldn't see client's information amid the evaluating procedure. The proposed technique evacuates the weight of cloud clients from costly inspecting work.

M. Suguna and S. Kindness Shalinie inspecting convention presents a put stock in outsider reviewer (TPA) will's identity accountable for checking the accuracy of information put away at distributed storage for the client without the requirement for recovering the whole information. The verification procedure in the proposed strategy diminishes the inspecting overhead at the cell phone utilizing short marks.

Anupriya.A.S, Ananthi, Dr. S Karthik proposed an updated methodology for securing the TPA by utilizing Keyed Hash Message Authentication Code (HMAC). Ms Bhavana Sharma presents the Elliptic Curve Cryptography (ECC) system. Her work likewise states ECC can be utilized as a part of versatile registering, remote sensor systems, and server based encryption, picture encryption and its application in each field of correspondence et cetera. Dispersed processing with ECC is an absolutely new territory and has enormous degree of research.

Nirmaljeet Kaur, Harmandeep Singh recommended that TPA is restricted to just giving the administration and utilizations hashing calculations for confirmation of information respectability and different calculations like AES, Blowfish for encryption and unscrambling.

Dalia Attas and Omar Batrafi proposed a model for securing information without giving it and transferring any protected information to the cloud.

K. Govinda, E Sathiyamoorthy strategy like Message Authentication Code [MAC] was utilized to confirm thrust worthiness of system.

III. PROBLEM STATEMENT

In cloud data can be store in large scale and which can be shared as well it means that a single database can be controlled or access by single or multiple users at same instance. The data can be accessed by user or group of user as well. The data owner plays an important role in these things that is owner will decide the access of data to TPA. In such system for TPA it's necessary to maintain the security and integrity of data. So that system is going to perform the privacy preserving on to the all data which is shared in group or with TPA for auditing .this will help to maintain data integrity for auditor and security over shared data.

IV. PROPOSED SYSTEM

The proposed system implementing various auto signature generation techniques over each and every file uploaded or share document by user with privacy preserving over cloud. In this TPA is able to maintain the auditing on the shared data and also check for data integrity without any information about user by using above techniques we can efficiently achieve followings.
(1) Public Auditing: The third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data.
(2) Correctness: The third party auditor is able to correctly detect whether there is any corrupted block in shared data.
(3) Unforgeability: Only a user in the group can generate valid verification information on shared data.
(4) Identity Privacy: During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

For distributed system to audit on the TPA we will use blind aggregrate forward (BAF) logging scheme as there are changes in the document signatures for documents for group of users. A set of cryptographic countermeasures have been proposed to enable secure logging on system .To develop the document signature of each document we will use the following algorithmns:-
1.3DES
2. MD-5/SHA
3. ECC
4. Digital Signature

- **Plan & Module:-**

Proposed system has some modules which are as given below:

- **Data Owner:** it is the user which is going to store their data on to the cloud and can share with the group members and access whenever its required.
- **TPA:** TPA (Third Party Auditor) is used to perform the public auditing on cloud based data and check the integrity and confidentiality of the user's data without accessing the entire file of data and generate auditing report for the data owner to know which group member access her file.
- **Cloud:** As we all know cloud is used to store the data in the same way we are going to not only store the data onto the cloud but also preserve the privacy of user's data by using privacy preserving system and user can access that data with specific authentication

- **Stepwise working of the Proposed System:**
  - Data owner login the system with his generated signature and upload the documents on the cloud.
  - Data owner can also modify the data after uploading the document and can share with other users or group members if he wants to share the data.
  - Provide security to the documents with the user signature and documents signature.
  - Update signature to the cloud server and by using TPA maintain the privacy of all documents.
  - TPA can access only the document information like size, no uses time, modification done by the user if any, last update etc, not the data.
  - User can access the document if and only if he has the valid verified signature provided by the data owner.
  - Maintain the data integrity and apply privacy preserving on the cloud storage.

V. About Work

The comparative analysis of different techniques and its disadvantages of different papers is given in the form of table is below:-

Table No.1:- Comparative Analysis of papers

Sr. No.	Paper Title	Authors	Year Of publishing	Methods Used	Limitations
1	Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud[7]	Boyang Wang, Baochun Li, , and Hui Li,	2014	Homomorphic authenticable signatures, not homomorphic signatures.	Signature schemes do not support blockless verification. Without blockless verification, the TPA has to download the whole data file to verify the correctness of shared data, which takes long verification times.
2	Dynamic Audit Services for Outsourced Storages in Clouds[8]	Devi Parvathy Mohan, K.J.Jagdish	2014	fragment structure, random sampling, and index-hash table (IHT)	It must requires external TPA monitoring. Not Secure
3	Provable data possession for securing the data from untrusted server[4]	S.Karthikeyan , J.praveen And Author Mrs. Sumathy	2015	Provable Data Possession (PDP)	The provable data possession is not capable for the source authentication technique. PDP is restricted form of the memory checking
4	Public key based third party auditing system using random masking & bilinear total signature for privacy in public cloud environment.[2]	J. Raja , Dr. M. Ramakrishnan	2017	public key auditing and random masking methods	Useful for group sharing but not performed on updation of documents.

VI. CONCLUSION & FUTURE WORK

Cloud computing provide the storage space and the related services to the user by its own CSP (cloud service provider) and day by day it grows fast and every organization use cloud to store data and access whenever it required, so the cloud is best to manage our data at the remote system. In this paper, for authentication, data integrity and group sharing we are using algorithmns 3DES,MD-5,ECC,digital signature and BAF.

In future we can use the cloud storage for storing our data and no need to worry about security issues. As the world grows technically day by day we require more security for the data and in future we can deploy this system for many organizations and maintain privacy of all confidential documents.

REFERENCES

[1]. Yanru Zhang, Xiang-Yang Li and Zhu Ha, "Third Party Auditing for Service Assurance in Cloud Computing", 78-1-5090-5019-2/17/$31.00 ©2017 IEEE

[2]. J. Raja , Dr. M. Ramakrishnan , "Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment", International Conference on Intelligent Computing and Control Systems ICICCS 978-1-5386-2745-7/17/$31.00 ©2017 IEEE

[3]. Nirmaljeet Kaur, Harmandeep Singh, "Efficient and Secure Data Storage in Cloud Computing Through Blowfish, RSA and Hash Function", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 4 Issue 5, May 2015.

[4]. S.Karthikeyan , J.praveen And Mrs Sumathy, "Provable data possession for securing the data from untrusted server", Int. Journal of Engineering Research and Applications, Vol. 5, Issue 3, (Part -2) March 2015

[5]. Subhas Chandra Sahana, Somen Debnath, Bubu Bhuyan, "A New Short Signature Scheme from Weil Pairing",

International Journal of Computer Applications (0975 – 8887) Volume 126 – No.14, September 2015

[6]. Kedar Jayesh Rasal, Dr. S.V.Gumaste, Sandip A. Kahate, "Survey on Privacy Preserving Public Auditing Techniques for Shared Data in the Cloud", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 3, May 2015.

[7]. Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "Oruta: Privacy- Preserving Public Auditing for Shared Data in the Cloud", IEEE 5th International Conference On Cloud Computing Year 2014.

[8]. Devi Parvathy Mohan, K.J.Jagdish, "Dynamic Audit Services for Outsourced Storages in Clouds", International Journal of scientific research and management (IJSRM), Volume 2, Issue 6, 2014.

[9]. Haritha Nuthi, Hemalatha Goli, Ramakrishna Mathe, "Data Integrity Proof for Cloud Storage", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 9, September 2014.

[10]. Nikita pathrabe, Deepali khtawar, "Ensuring Data Storage Security in Cloud Computing", International Journal of Research in Advent Technology, Vol.2, No.2, February 2014.

[11]. Hadassa Katta, Vivek Kolla, P Raja Rao, "Scalable and Efficient Provable Data Possession", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.

[12]. Yihua Zhang and Marina Blanton, "Efficient Dynamic Provable Possession of Remote Data via Balanced Update Trees", ASIA CCS'13, May 8–10, 2013.

[13]. Rampal Singh, Sawan Kumar, Shani Kumar Agrahari, "Ensuring Data Storage Security in Cloud Computing", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013.

[14]. Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, Michael stergaard Pedersen, "Practical Short Signature Batch Verification", University of Illinois at Urbana-Champaign, January 21, 2009.

[15]. Hovav Shacham and Brent Waters, *"*Compact Proofs of Retrievability*"*, in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008.

[16]. Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song, "Provable Data Possession at Untrusted Stores", CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA. Copyright 200ACM.

[17]. Giulia Traverso, Denise Demirel, and Johannes Buchmann, "Homomorphic Signature Schemes - A Survey".

[18]. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, *"*Privacy-Preserving Public Auditing for Secure Cloud Storage".

[19]. Dan Boneh, Craig Gentry, Ben Lynn, Hovav Shacham, "*Aggregate and Veri_ably Encrypted Signatures from Bilinear Maps*".

[20]. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "*Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing*".

[21]. Giulia Traverso, Denise Demirel, and Johannes Buchmann, "*Homomorphic Signature Schemes - A Survey*".

[22]. Ronald L. Rivest, Adi Shamir, and Yael Tauman, "*How to Leak a Secret*".

[23]. Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "*Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*", This research was supported in part by NSF ITR/Cybertrust grants 0456717 and 0627781.