Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.381 – 388

RESEARCH ARTICLE

Enhanced Privacy Preserving with Traceability on Collective Data Stored in Cloud

D.Sugumar[1], T.Tholhappiyan[2], D.K.Karthika[3]

[1]*Department of CSE, Ranganathan Engineering College, Coimbatore, Anna University, Chennai, India*
[2]*Department of CSE, Ranganathan Engineering College, Coimbatore, Anna University, Chennai, India*
[3]*Department of CSE, Ranganathan Engineering College, Coimbatore, Anna University, Chennai, India*

[1] sugumar.ds@gmail.com, [2] tholhappiyanit@gmail.com, [3] karthikaprakash89@gmail.com

***Abstract** - Cloud computing is open and unrestricted, reliability of data and delivery became the prime indicators. Cloud became a much bigger trend in the business and networking world. This also provides flexibility so it is very useful in a new generation of services and products. Normally, the data is stored and shared to multiple users. The data can easily lose, dropped or corrupted due to software fault or network failures. There are lot of technologies are used to allow public verifiers to audit cloud data without retrieving entire data or file. Oruta is one of technology that uses ring signature, used to compute and verify metadata needs to audit the correctness of shared data in the block. In this paper, we propose a new mechanism that is improves the privacy of data that achieves traceability with data freshness.*

Keywords- Cloud Computing, grouping, traceability, data freshness, signature

1. INTRODUCTION

Cloud computing and cloud services capture new behavior of idea about computing architecture and delivery models. Within cloud, everything becomes a service so that companies can create new initiatives without a massive upfront investment. Cloud computing offers unique and new business profits and will help to change the way businesses operate, collaborate, and compete [1]. The cloud is the next stage in the evolution of the Internet. It provides everything from computing power to business processes to personal collaboration is delivered to you as a service wherever and whenever you need it.

Fig 1: Cloud Computing

Cloud computing supports to reduce or cut capital and operational costs. The IT departments are searching the way to store all data in data center for easy to share. A 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality of service [2].

Cloud computing can provide resources dynamically at any time. One of the major and important attribute of cloud computing is scalability, which is achieved through the server virtualization. Normally, the data is stored and shared to multiple users. The data can easily lose, dropped or corrupted due to software fault or network failures [3] [4].

1.1 Key Features Of Cloud Computing

The most talking term on currently in the IT industry is the cloud computing. Everyone is think about features of cloud like cost benefits, security and privacy. Some of the features are explained in below.

Elasticity- The size of the data location is should be changed appropriately and quickly with the time of demand. So the cloud should provide flexible (elastic) size. i.e., how much size the user want.

On-demand and Self Services- The cloud should allows the users to perform the tasks like building, scheduling, deploying and managing.

Pricing- No up-front cost for deployment. It is completely based on the usage i.e., pay per use concept.

Quality of Service- Cloud computing is must provide best service level to customers or users. Service level agreements also include guarantees, availability, performance and bandwidth.

Some other features and benefits of cloud computing are shown in figure 2.

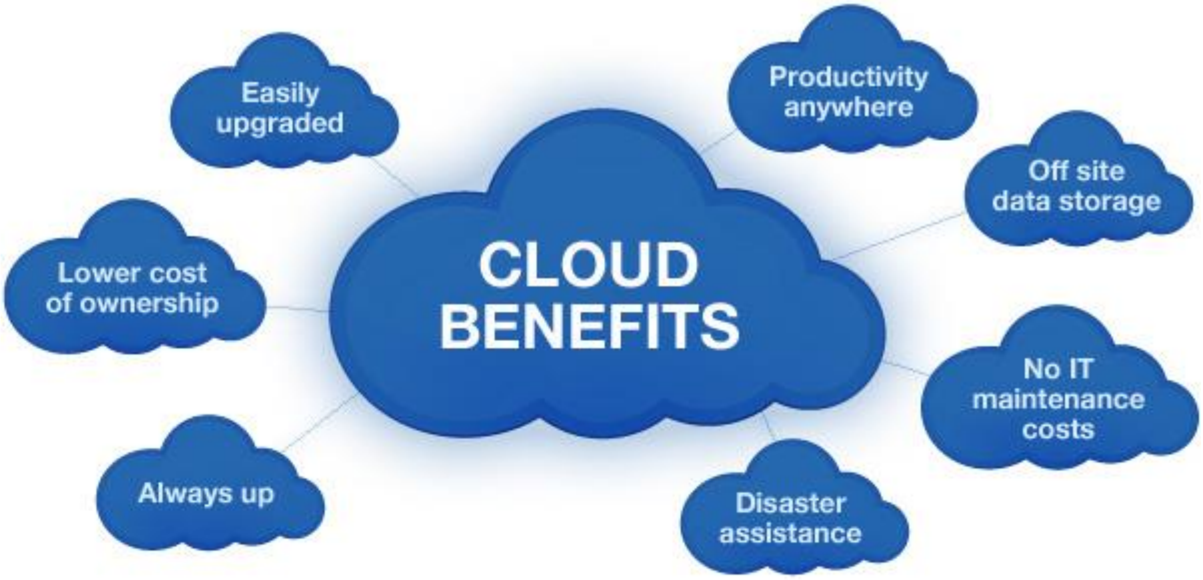

Fig 2: Benefits of Cloud computing

2. PROBLEM STATEMENT

Cloud computing is gives flexibility to the users and customers. Users pay as much as they use. Users don't need to set up the large computers but the operation is managed by the Cloud Service Provider (CSP). The user gives their data to CSP; CSP has control on the data. The user needs to make sure the data is correct on the cloud. Internal (some people on CSP) and external (hackers) threats are available for data integrity.

Cloud service providers (CSP) offer users efficient and scalable data storage services to users and public verifiers [5]. There are lot of cloud service providers (CSP) are available including Google drive, Sky drive, Dropbox, iCloud, etc., Basically checking of data correctness is works under retrieve the entire data or file from the cloud. And then verify the data integrity by checking the correctness of signatures of entire data. It can use algorithms like RSA [6] or MD5 [7] (using hash values). These RSA and MD5 algorithms are get entire data for checking correctness. The main problem is the size of cloud data is large in general. So downloading the entire cloud data is take long time, and to verify data integrity will get high commutation cost.

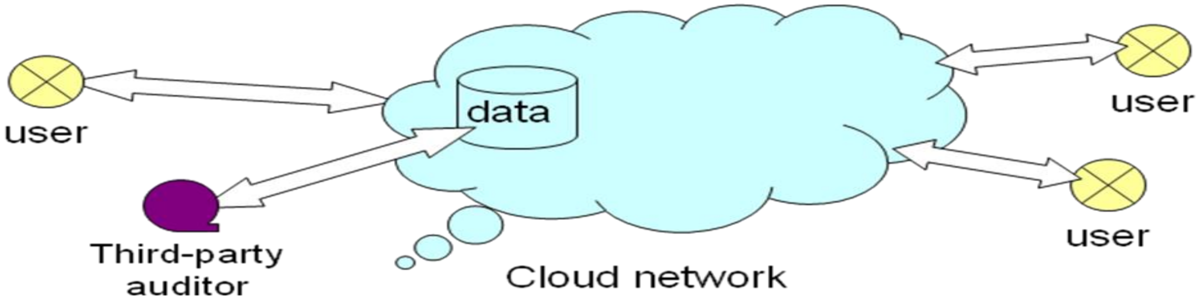

Fig 3: Cloud network with third party auditor (TPA)

The stored data in cloud can be used by researcher (i.e., public verifier) via third party auditor (TPA). So the confidential information will be used by public verifiers easily.

3. EXISTING SYSTEM APPROACH

Today’s many more uses of cloud data like, Data mining and machine learning do not need to download the entire cloud data to local devices [5] for data verification. In recent times, many mechanisms like WWRL [8], Provable Data Possession [9] and Dynamic Provable Data Possession [10] are used to allow public verifiers for data correctness without retrieving the entire data or file.

ORUTA (One Ring to Rule Them All) [11] is a new privacy preserving public auditing mechanism for shared data in the cloud. This is allows public verifiers to audit cloud data without retrieving entire data or file. Oruta can be uses the ring signature. The concept of the ring signatures was first proposed by Rivest et al. [12] in 2001. With a ring signatures, a verifier sure that a signature is computed using one of group members’ private keys, but the verifier is not able to determine which one.

A new Homomorphic Authenticable Ring Signature scheme is used called HARS, which is extended from a classic ring signature scheme [13]. The ring signature is generated by HARS are not only able to preserve identity of privacy but also capable to support blockless verifiability. HARS contains three different algorithms: KeyGen, RingSign and RingVerify. In KeyGen, every user in the group creates his/her public key and private key. In RingSign, a user in the group is able to create a sign on a block and its block identifier with his/her private key and all the group members’ public keys. A block identifier is a string that can distinguish the corresponding block from others. In RingVerify, a verifier is able to check whether a given block is signed by a group member or not.

HARS is used to identify the singer of each and every block in shared data that is kept private from public verifiers without retrieving the entire data or file in cloud.

In figure 4 contains three parties. They are users, cloud server and public verifier. It also contains two types of users called original user and group members. Each and every member can easily access and modify the cloud data. There are two types of data also available in cloud. They are shared data and verification metadata. The verification metadata is called signatures. First the public verifier can send the auditing challenge to the cloud server. And cloud server send the auditing proof of the shared data. Then public verifier checks the correctness of entire data by verifying the correctness of the auditing proof.

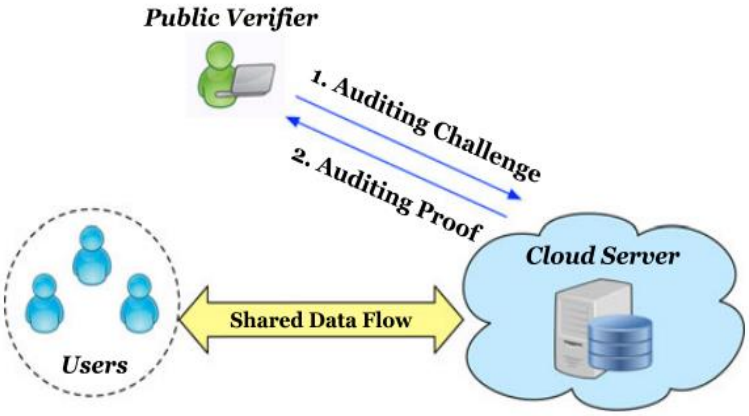

Fig 4: Existing system model

Drawbacks of Oruta

The main advantage of oruta is to perform multiple auditing simultaneously rather than one by one. But it contains some following drawbacks:

1. Traceability is still not achieving when someone in the group is misbehaved.
2. Its fails to scale to a large number of users sharing data in a group
3. Time taken is increasing linearly when the number of users increased in a group.
4. Can't prove the data freshness.

4. PROPOSED SYSTEM (OR) RELATED WORK

We propose a new technique called Group Oriented Ring Signature (GORS also called Knox), is a privacy-preserving public auditing mechanism for data stored in the cloud and shared among large number of users in a group. In particular, we operate group signatures to construct the homomorphic authenticators. So that a third party auditor (TPA) verify the integrity of shared data for users without retrieving the entire data or information. The Group Oriented Ring Signature is identify the signer on each and every block in shared data is kept private from the TPA (public verifiers) without retrieving entire data. In this technique, the amount of shared information used for verification, also the time it takes to audit are not affected by the number of user's increases in the group but cannot reveal the identities of signers on all blocks in shared data. In addition, this proposed system exploit homomorphic MACs to reduce the size used to store such verification information.

4.1 Construction of HAGS

Following are the general constructions of group signatures in [14, 15], HAGS (Homomorphic Authenticable Ring Signature) contains five main algorithms: **KeyGen, Join, Sign, Verify and Open**. In **KeyGen**, the group manager (original user) can generates her private key and group public key. In **Join**, the original user, who creates and shares the data in the cloud is called group manager, is proficient to add new users into group without recomputing any verification information in cloud. A group user can generate signature using her private key and the public key in the **Sign**. In **Verify**, the verifier is able to check the correctness of the data using the group public key, but she cannot reveal the identity of the signer. **Open**, the original user may trace the group signatures on shared data, and reveals the identities of signers at what time it is necessary.

4.2 Secret sharing algorithm

We allow the third party auditor (TPA) to share a secret key pair with users, which we refer to as authorized auditing. Although we also allow the authorized TPA to possess the secret key pair, the TPA cannot compute the valid group signatures as group users because this secret key pair is only a part of a group user's private key. To our best knowledge, we used Secret sharing algorithm for sharing secret keys with authorized

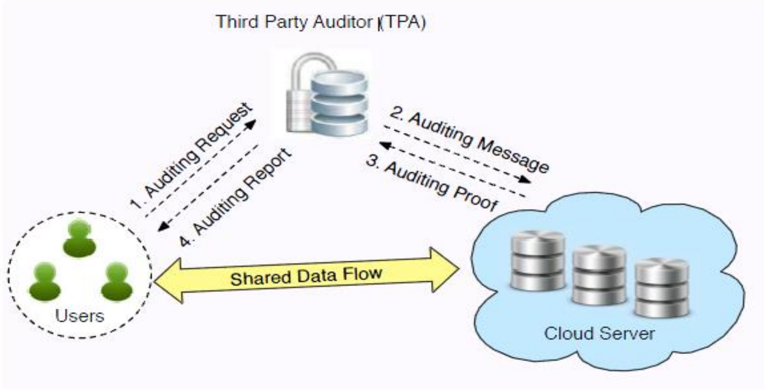

Fig 5: Cloud model with Secret sharing algorithm

user. In figure 5 shows the security of our proposed system. So the Secret sharing algorithm allows user to share confidential information to particular another user. This information is cannot viewed by public verifiers.

4.3 Traceability

Group signatures are first introduced by Chaum and van Heyst [16]. Aim is to provide anonymity of signers, who are from a same group. A public verifier is convinced that messages are correct and signed by one of the group members, but that cannot reveal the identity of the signer. Only the group manager (original user) is able to trace these group signatures and reveal the identity of the signer.

The original user, who acts as the group manager, is able to trace the identity of the signer on each block using her group manager's private key. The high level comparison between Group Oriented Ring Signature (GORS) and other previous methods are shown in Table 1.

Methods / **Features**	PDP [9]	WWRL [8]	Oruta [11]	GORS
Public Auditing	✓	✓	✓	✓
Data Privacy	✗	✓	✓	✓
Identity Privacy	✗	✗	✓	✓
Traceability	✗	✗	✗	✓

Table 1: Comparison among Different Mechanisms

In particularly, when size of the group is 100, GORS is able to finish an auditing task in less than 4 seconds while Oruta is requires nearly 12 seconds finishing that same auditing task. The other benefits comparison is shown in below table 2.

	Oruta [11]	GORS
Data Storage Usage (GB)	2	2
Signature Storage Usage (GB)	2	0.33
Communication Cost (KB)	18	106.4
Auditing Time (seconds)	11.49	3.44

Table 2: Comparison of Auditing Performance

5. CONCLUSION AND FUTURE WORK

In this paper we propose a novel method called Group Oriented Ring Signature (GORS). It is a privacy preserving public auditing mechanism for data stored in the cloud and shared among large number of users in a group. The original user is be able to trace the identity of the signer on each block.

GORS is solves some of the drawbacks of oruta. But still data freshness is not proved by GORS. In future work we analysis new technique or algorithm to prove the data freshness in the cloud.

ACKNOWLEDGEMENT

I would like to extend by gratitude to my guide Mr. T. Tholhappiyan for his support guide for assisting me in this paper work.

REFERENCES

[1] Judith Hurwitz, Robin Bloor and Marcia Kaufman, “Cloud Computing For Dummies,” Wiley Publishing, Inc., Indianapolis, Indiana – 2010.

[2] Keith Jeffery and Burkhard Neidecker-Lutz, “The future of Cloud computing,” Opportunities for European Cloud Computing Beyond, 2010.

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

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

[5] 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.

[6] R.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” Comm. ACM, vol. 21, no. 2, pages 120-126, 1978.

[7] The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/html/rfc1321, 2014.

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

[9] G.Ateniese, R.Burns, R.Curtmola, 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.

[10] C.Erway, A.Kupcu, C.Papamanthou and R. Tamassia, “Dynamic Provable Data Possession,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), pp. 213-222, 2009.

[11] Boyang Wang, Baochun Li, and Hui Li, “Oruta: Privacy-Preserving Public Auditing For Shared Data In The Cloud” IEEE transactions on Cloud Computing, vol. 2, no. 1, pages 43-56, January-March 2014.

[12] R.L.Rivest, A.Shamir and Y.Tauman, “How to Leak a Secret,” Proc. Seventh Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT’01), pp. 552-565, 2001.

[13] D.Boneh, C.Gentry, B.Lynn and H.Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT’03), pp. 416-432, 2003.

[14] G.Ateniese, J.Camenisch, M.Joye and G.Tsudik, “A Practical and Provably Secure Coalition-Resistant Group Signature Scheme,” In: Proc. CRYPTO., pp. 255–270, Springer-Verlag, 2000.

[15] D.Boneh, X.Boyen and H.Shacham, “Short Group Signatures,” In: Proc. CRYPTO., pp. 41–55. Springer-Verlag, 2004.

[16] D.Chaum and van E.Heyst, “Group Signatures,” in Proc. EUROCRYPT., pp. 257–265. Springer-Verlag, 1991.