Privacy-Aware Public Auditing System for Shared Cloud Data with Dynamic Groups

A.Pramod kumar[1], G.Shyama Chandra Prasad[2]
[1]*Assistant Professor, Matrusri Engineering College, Hyderabad, T.S, India*
[2]*Associate Professor, Matrusri Engineering College, Hyderabad, T.S, India*

***Abstract*- Today, cloud storage turn out to be one of the critical services, because users can easily amend and share data with others in cloud. However, the integrity of shared cloud data is vulnerable to inevitable hardware faults, software failures or human errors. In this paper, we propose a new privacy-aware public auditing mechanism for shared cloud data by making a homomorphic valid group signature. Nothing like the existing solutions, our plan requires at least team professionals to recover a track key cooperatively, which removes the mistreatment of single-authority ability and provides no flammability. Furthermore, our scheme means that group users can trace data changes through the specified binary tree; and can recover the latest right data stop when the existing data stop is destroyed. Also, the formal security analysis and investigational results reveal that our system is probably secure and efficient.**

***Index Terms*-Data Integrity, Homomorphic Verifiable, Nonframeability, Provable Security.**

I. INTRODUCTION

Cloud computing is a distributed computing paradigm which is able to host and offer a variety of net-based services for the clients. In current years, the cloud computing utilization price has extended unexpectedly because of the exclusive benefits furnished by way of the cloud. These blessings encompass adopting the pay-as-you-cross precept as a pricing model, providing as a lot of assets as wanted which achieves an excessive degree of scalability, saving the efforts and cash had to hold the IT infrastructure, and decreasing the charges and dangers of launching an funding in which the consumer isn't obliged to spend lots of money to construct the required infrastructure. All of these advantages attracted many enterprises to rely on the cloud infrastructure instead of the in-house infrastructure [1, 2].

Among the services furnished through the cloud is garage as a service which lets in the users to save, to remotely manage and to get entry to their information over the net. From the users' the factor of view, along with IT organizations and character customers, cloud storage carrier has completed a set of attractive blessings which incorporates disposing of the load of statistics storage management from the customers' shoulders, smooth statistics get admission to through the internet regardless the modern geographical locations, saving the cash needed for the software, hardware, and renovation, and many others [3]. However, there is a set of challenges and research problems which got here with cloud garage provider and want to be alleviated to boom the consumer's contentment of this carrier. One of those issues is the customers' concern about the integrity and availability in their records and their feelings that the facts can be accessed or modified by means of external intruders due to the restricted manage granted to the customers over the faraway cloud nodes. This worry from the customers may be justified when we recognize that security threats and service outages are occurring for the cloud services from time to time [4]. Also, there are numerous motives that could encourage the cloud service company to act inappropriately closer to the outsourced statistics such discarding the records of a person for financial reasons, hiding the safety breaches which affected the facts to save their reputation [5, 6]. Hence, there is no assure the availability and integrity of facts [4].

Therefore, data auditing has been evolved to allow the users to use the cloud storage as they use their local storage without worrying about the integrity of their data. Users can perform data auditing mission

by themselves (private auditing) or they can exploit the expertise, knowledge, capabilities, and professional skills of an independent entity called Third Party Auditor (TPA) (public auditing) rather than putting the burden of the auditing task on the users' shoulders [4, 7]. It is necessary that the TPA should be able to audit the data without knowing its contents to the preserve the data privacy. Also, the data availability can be achieved through storing the data of users on multi-cloud instead of a single cloud.

II. RELATED WORKS

In [4], they proposed a public auditing method which can be performed by a TPA while preserving the privacy of data which stored on the cloud nodes. Their proposed method is based on random masking and homomorphic linear authenticator to make the TPA know nothing about the content of data during the auditing process. Also, they designed the TPA in such a way that makes it able to handle many auditing requests from multiple users on the same time in a batch manner.

In [8], the researchers have developed a mechanism for the public auditing service through a TPA while preserving the privacy of data. Their proposed mechanism has utilized ring signature for computing the verification information required to verify the integrity of the shared data. TPA cannot recognize the identity of the person who signed on each data block. Also, the authors in [9] proposed another public auditing scheme to verify the integrity of the shared data which reside on the cloud. In their proposed method they support dynamic operation on data and group dynamic. Also, they decreased the computation burden put on the users through employing a proxy signature. On the same time, by adopting a Lagrange interpolating polynomial, the proposed method achieves the identity's privacy-preserving while keeping the communication overhead and computation cost small as possible. Toward achieving the same goals, in [7] a public auditing scheme has been developed with design goals to verify the integrity of data along with confidentially, be privacy preserving, be efficient, and be secure. Their proposed auditing scheme employed AES cipher for encryption, SHA-2 for checking the data integrity, and RSA for calculating the digital signature.

Another public auditing scheme is suggested in [10] for monitoring data insertions, modifications, and deletions. The suggested scheme supports data dynamics and performs the auditing process by using multiple TPA. In addition to the ability of the suggested scheme to handle many auditing requests from multiple users at the same time through batch auditing, they used the concept of ring signatures besides improving block level authentication by using Merkle Hash Tree.

In [11], a public auditing scheme has been devised which performed by a TPA while preserving data privacy with efficient computation. Their solution is based on Chinese Theorem Remainder preceded by a cryptographic hash function with an attempt to optimize the computation at cloud server, TPA, and the owner of data. Also, another public auditing mechanism has been proposed in [12] for educational multimedia data stored in the cloud storage which allows fully dynamic auditing. They guarantee the privacy of data through utilizing a homomorphic hash function and random values beside its immunity against temper attack and lose attack.

In [13], a privacy preserving public auditing mechanism called Knox has been proposed for data maintained in the cloud storage in which there a large number of users who can access the data. In order to build homomorphic authenticators, Knox adopts group signatures which allow the TPA to perform the auditing process without the need for retrieving the whole data and without revealing the identity of the signer. The results have been shown that the amount of time and information required for the verification process are not influenced by the number of users. At last but not least, the researchers in [14] have combined public verification with ID-based aggregate signature to build data integrity checker protocol. Besides performing the auditing process on behalf of the data owners, the proposed mechanism can reduce the overhead of checking tasks based on the identities of users.

III. THE PROPOSED APPROACHES

As shown in Fig. 1, the system model contains four entities: cloud, TPA, trusted private key generator (PKG), and group users. The cloud has powerful storage space and computing capacity, and provides

services (e.g., data storage, data sharing, etc.) for group users. The TPA can verify the integrity of the shared data on behalf of the group users. The PKG generates the system public parameters and group key pair for group users. The group users include two types of users: GMs (Group Managers) and ordinary members.

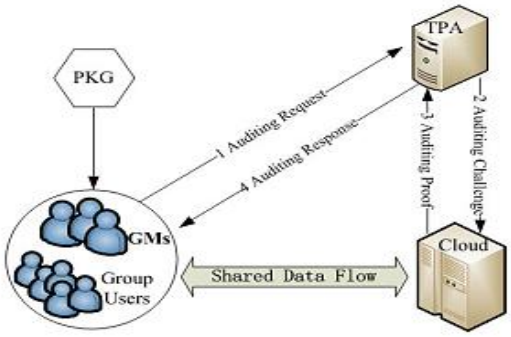

Figure 1: The system model of NPP

1) Integrity Threat. There are two kinds of threats related to shared data integrity. One is that external attackers might corrupt the shared data in the cloud so that group users can no longer access the correct data. The other is that the cloud may corrupt or delete the shared data due to the hardware/software faults or human errors. What's worse, the cloud may conceal the fact of data damage from users to maintain self-interest and service reputation.

2) Privacy Threat. As a trusted and inquisitive verifier, a TPA might obtain some privacy information from the verification metadata during the auditing process. For instance, the TPA might analyze which data block has been modified most or which user has modified the data most, and finally conclude which particular data block or which group the user is of a higher value than the others. Then the TPA might directly obtain the data or the identity of the group user from the signatures of the data blocks.

3) Challenge Threat. Because the auditing challenge message is straightforward and has not been authorized, any other entity can utilize the TPA to contest the cloud for auditing proofs. In this case, a malicious entity might launch denial of service attacks on the cloud by sending massive challenge messages continuously, which will lead to network congestion and unnecessary waste of the resources of the cloud.

To reap integrity checking of the shared facts inside the cloud, NPP is expected to the subsequent design objectives:

1) Public auditing: Besides the group customers, the TPA can also efficiently take a look at the integrity of the shared facts in the cloud without retrieving entire customers' statistics from the cloud.

2) Authorized auditing: Only the TPA that has been authorized via the group customers can task the cloud.

3) Identity privacy: During the method of auditing, the TPA can not examine the identification of the organization consumer from the signatures of the information blocks.

4) Traceability: Under positive conditions, the organization managers can reveal the signer's identity from the signatures and determine which group person has changed the information block.

5) Nonflammability: Group managers can assure the equity of the tracing system, i.e., innocent institution person will not be framed, and the institution managers will not harbor the misbehaved person.

6) Support information traceability and recoverability: Group customers can without difficulty hint the facts modifications and recover the trendy accurate statistics once modern data is damaged.

7) Support institution dynamics: Group dynamics consist of two elements. One is that GMs can effortlessly be a part of or go away the organization, the other is that new customers may be without problems added into the organization and misbehaved customers can be efficaciously excluded from the panel.

Group Managers Dynamics:

• GM joining

If a new GM wants to adhere to the group, the PKG computes $S' = S+1$, and tests whether $2t-1 \geq S'$. If it holds, the PKG will calculate a new piece (S', Xs') with polynomial f(x) and distribute it to the new GM′ S ; otherwise, the PKG chooses a new $(t'-1)$-degree polynomial $f'(x) = b'0 + b'1x + \cdots + b't'-1x t'-1$, where $2t'-1 \geq S'$, $b'0 = X$, $b'1, \cdots, b't'-1 \in Zq$, and computes $X'l = f'(l)(l = 1, 2, \cdots, S')$, i.e. X is divided into S' pieces $X'l$ and then distributed to GMl . Also, the PKG generates a new key pair {spk', ssk'}, and broadcasts it to all the GMs, who can then share it with the existing group users. Note that the process of updating {spk, ssk} does not affect auditing, because the signing keys, the membership keys and the revocation keys of the

existing users do not need to be updated. Nor do the signatures of the data blocks.

• GM leaving: If an existing GMl wants to leave the group, the PKG first sets $S' = S - 1$, chooses a new $(t' - 1)$-degree polynomial $f'(x) = b'0 + b'1x + \cdots + b't'-1x t'-1$, where $2t' - 1 \geq S'$, $b'0 = X$, $b'1$, $\cdots$, $b't'-1 \in Zq$, and then computes and distributes new $X'l = f'(l)(l = 1, 2, \cdots, S')$ to each GMl . Also, the PKG generates a new key pair {spk', ssk'}, and broadcasts it to all the GMs, who can then share it with the existing group users.

2) User Revocation: GMs maintain a users list, which is composed of each user's related key and expiration time. Once a user's service subscription expires, their signing key should become invalid from then on. In this case, any GM can invoke the Revoke algorithm by updating the membership information Ω and the key pair {spk, ssk} and setting the value of the revoked user's expiration time to be negative. There might be misbehaving users in the group. In this case, any GM can invoke the Revoke algorithm as mentioned above. Note that when a user is revoked from a group, GMs do not need to re-compute and re-distribute new keys to the valid users, since the revoked user Ui cannot find f, $b \in Zq$ such that $f \cdot u + b \cdot rvki = 1$, Ui cannot compute the partial signature V2 anymore. If the revoked user Ui maliciously reveals their signing key uski = (xi , π), then the partial signature of other users can be discerned because of the common key π. However, it is not enough to forge a valid signature as the secret key xj of the other users is still unknown. Therefore, the partial signature V1 cannot be computed. As we have demonstrated, valid users do not need to update their keys and the existing signatures.Signatures belonging to the revoked users can be recomputed by the GMs. Specifically, the existing user interacts with GMs to generate a proxy signature key; then GMs use the proxy key to compute the signatures of the revoked users. That transforms them into the signatures which sign by the private key of the existing user.

IV. CONCLUSION

In this paper, we propose a singular multi-degree privacy is keeping public auditing scheme for cloud data sharing with multiple managers. During the process of auditing, the TPA cannot attain the identities of the signers, which ensures the identification privateness of the institution customers. Moreover, not like the prevailing schemes, the proposed NPP calls for as a minimum t group managers to work collectively to trace the identity of the misbehaving consumer. Therefore, it removes the abuse of unmarried authority strength and ensures no-frame capability. Exceptionally, organization customers can hint the facts adjustments thru the designed binary tree and get better the cutting-edge accurate records block while the modern facts block is broken. Also, the analysis and the experimental results display that NPP is probably at ease and efficient.

REFERENCES

[1] Zhang, Q., Cheng, L. and Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), pp.7-18.

[2] Malik, S., Huet, F. and Caromel, D., 2012, December. RACS: a framework for resource aware cloud computing. In Internet Technology And Secured Transactions, 2012 International Conference for (pp. 680-687). IEEE.

[3] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I. and Zaharia, M., 2009. Above the clouds: A berkeley view of cloud computing.

[4] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z. and Song, D., 2007, October. Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 598-609). ACM.

[5] Wang, Q., Wang, C., Li, J., Ren, K. and Lou, W., 2009, September. Enabling public verifiability and data dynamics for storage security in cloud computing. In European symposium on research in computer security (pp. 355-370). Springer Berlin Heidelberg.

[6] Wang, C., Chow, S.S., Wang, Q., Ren, K. and Lou, W., 2013. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on computers, 62(2), pp.362-375.

[7] More, S. and Chaudhari, S., 2016. Third Party Public Auditing Scheme for Cloud Storage. Procedia Computer Science, 79, pp.69-76.
[8] Wang, B., Li, B. and Li, H., 2014. Oruta: privacypreserving public auditing for shared data in the cloud. IEEE transactions on cloud computing, 2(1), pp.43-56.
[9] .Zhang, J.H. and Zhao, X.B., 2015. Privacypreserving public auditing scheme for shared data with supporting multi-function. J. Commun, 10(7), pp.535-542.
[10] Bhagyashri, S. and Gurav, Y.B., 2014. Privacypreserving public auditing for secure cloud storage. IOSR Journal of Computer Engineering (IOSR-JCE), 16(4), pp.33-38.
[11] Dang, H.V., Tran, T.S., Nguyen, D.T., Bui, T.V. and Nguyen, D.T., 2015. Efficient privacy preserving data audit in cloud. In Advanced Computational Methods for Knowledge Engineering (pp. 185-196). Springer International Publishing.
[12] Kim, D., Kwon, H., Hahn, C. and Hur, J., 2015. Privacy-preserving public auditing for educational multimedia data in cloud computing. Multimedia Tools and Applications, pp.1-15.
[13] Wang, B., Li, B. and Li, H., 2012, June. Knox: privacy-preserving auditing for shared data with large groups in the cloud. In International Conference on Applied Cryptography and Network Security (pp. 507-525). Springer Berlin Heidelberg.
[14] Tan, S. and Jia, Y., 2014. NaEPASC: a novel and efficient public auditing scheme for cloud data. Journal of Zhejiang University SCIENCE C, 15(9), pp.794-804.