Secure Cloud Storage through Public Auditing and Cryptographic Primitives.

Ganesh mouli Bandari [1], N. Subhash Chandra[2] ,V.Krishna[3]

1pursuing M.Tech (IT), Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India
2working as Professor (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU-Hyderabad, A.P, India
3working as Associate Professor & HOD (IT Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India

***Abstract*— The purpose of Cloud Computing is a long dreamed vision of computing as a utility, where user want to store their data remotely into the cloud and so as to enjoy the on demand of high quality application and services for the shared pool of configurable computing storage of outsourcing data so users can be relieved from the burden about local storage and maintenance of data. However, in general the users have no longer physical possession of large size of outsourcing data makes data integrity protection in Clouding and a very challenging , potentially formidable task, this is for users especially with constrained resources and capabilities of cloud computing. And to enabling public availability of cloud stored data for security of critical importance of users and they can resort to an external third party to check the integrity of user outsourced data when user needed. To securely introduce an effective third party auditor (TPA), the following of two main requirements have to met:**

1) TPA has to work efficiently to audit the cloud data storage without local copy of data demanding, and no need of additional on-line burden to the cloud user.

2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper we combine the public key based HomoMorphic authenticate with random masking to achieve the privacy-preserving public cloud data auditing system, for to meet all the above requirements.

***Keywords*— Data storage, privacy-preserving, public audit ability, cloud computing and delegation**

I. INTRODUCTION

Cloud Computing has been involved as the next generation information technology due to its long list of unprecedented advantages in the IT history: on-demand self service and ubiquitous network access, location independent resource pooling of rapid resource elasticity and usage-based pricing and transference of risk [2]. As a disruptive
technology now Clouding is transforming the very nature of how to use for businesses use information technology. The main fundamental aspect of this paradigm shifting is that data is being centralized or outsourced in to Cloud. From user perspective, involving of IT and individuals enterprises, storing data remotely in cloud in a flexible on-demand manner and it brings appealing benefits: relief to the burden for the storage management, mainly the data access universally by location independence, and for the avoidance of total capital expenditure on hardware, and software, and for personnel maintenance also, etc [3]. Cloud Computing (CC) makes these advantages more appealing than ever to the users, and it brings new challenging security threats towards outsourced data users.

Since the cloud service providers (CSP) are different administrative entities of data outsourcing and it makes actual relinquishing user's ultimate control over the fate of their data. The correctness of the stored data in the cloud is being put at risk in some of following reasons. First of all the infrastructure under the clouds are much more powerful and reliable than the personal storing data computing devices, even though still they are facing the broad range of both internal and external attacks for data integrity [4]. For example of outsourcing and security breaches of note worthy cloud services appear in a form of time to time process [5], [6], [7]. Secondly, To exist various motivations for CSP has unfaithfully behavior towards the cloud users about their outsourced data. For examples, CSP might reclaim the storage for monetary reasons by discarding data that has not been accessed or even hide stored data and loss incidents to maintain a reputation [8], [9],[10]. It's in short, although out stored data in the cloud is economically attractive for long-term and large-scale of storage, and it does not immediately offer any guarantee on stored data integrity and availability. This is main problem, if it does not properly addressed the user may impede the success of cloud architecture. How users no longer physically possess their own data to storage, so the traditional cryptographic primitives for the security purpose of data protection and it can't directly adopted [11]. In particular, to download all the data simply for its integrity verification is not a practical solution but due to the expensiveness in I/O transmission it cost across the network. Besides, even it's often insufficient to find the data corruption when accessing the data, so in this case the cloud may not give users correctness assurance for the un-accessed data and might be too late to recover the loosed data or damage data. Considering the very large size of the outsourced data and the

user's constrained resource capability, so the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users [12], [8]. Moreover, the overhead of using cloud storage should be minimized as much as possible to the user and he does not need to perform all the operations to use the data. In general user doesn't want to go through all these complexity to verifying the data integrity. Besides, if in case one user accesses the same cloud storage, say in an enterprise setting. For the easier management, it can be desirable that cloud only entertains verification request from a single designated party. To ensure the data integrity fully and save the cloud users data computation resources as well as online burden to reduce, it is the main critical importance to enable public auditing service for cloud storage data then users may resort to another third party auditor (TPA) to audit the outsourced user data when they needed. The TPA, who has expertise it and capabilities that the users may not, s they can periodically check the integrity of all storage data in cloud on behalf of the users, which can provides a much more easier and affordable way for the users to ensure their total storage correctness in the cloud server. Moreover, in addition to help the users to evaluate the risk of their subscribed cloud data services, the audit result from third party would also be beneficial for the cloud service providers to improve their cloud based service platform and to support them, and even though to serve for independent arbitration purposes [10]. In a word, so to enabling the public auditing services plays an important role for the cloud economy to become fully established, where the users want to access the risk and gain trust in the cloud.

Now we use experiment to justify the efficiency of our recursive binary search approach for TPA to sort out the invalid responses when batch auditing fails, as discussed in Section III-D. This experiment is tightly pertained to work in [20], which evaluates the batch verification efficiency of various short signature schemes. To evaluate the feasibility of the recursive approach, we first generate a collection of 256 valid responses, which implies the TPA may concurrently handle 256 different auditing delegations. We then conduct the tests repeatedly while randomly corrupting an α-fraction, ranging from 0 to 20%, by replacing them with random values. The average auditing time per task against the individual auditing approach is presented here The result shows that even the number of invalid responses exceeds 15% of the total batch size, the performance of batch auditing can still be safely concluded as more preferable than the straightforward individual auditing. Note that the random distribution of invalid responses within the collection is nearly the worst-case for batch auditing. If invalid responses are grouped together, it is possible to achieve even better results.

II. PROPOSED WORK

In existing system they concern about auditing of cloud with third party auditor. In existing approach they check about only the cloud authenticity. We know that cloud is an open environment where any end party can store and fetch the data. By using the auditing system cloud trustiness can be verified, but there may be a chance that any intruder will attack on cloud and harm the user data .In this case the auditing system only will not be efficient for preserving the privacy of user data. In this paper we are proposing a system which having mainly two phase. In the first phase the auditing of cloud will check and if the cloud is verified by our auditing system then we will encrypt the user data to provide the security of data over cloud and store the data into the cloud. This proposed system is efficient for auditing of cloud and data privacy preservation also.

This section of process presents public auditing scheme which can provides a complete outsourcing solution of data to the users not only the data itself, and also its integrity checking. After interaction of notations and brief preliminaries, we start from a small overview of our public auditing system and after discuss two main forwarding schemes and their demerits. Then after we can present our main scheme and it shows how to extent our main scheme to support batch auditing for the TPA upon delegations from any number users. Overall, we discuss how to generalize our privacy-preserving public auditing scheme and its support of data dynamics. In this proposing scheme we embed a third party auditor for auditing purpose and making this third party auditor more efficient as compare to existing approach for auditing and storing the data by using cryptographic primitives. By implementing this schema we can get a secure and trusted cloud for storing the cloud.

To enable the privacy preserving in public auditing for the cloud data storage under the aforementioned model, and our protocol design can achieve the following security and performance should be guarantee and public audibility to allow the TPA to verify validation of the cloud data on demand without retrieving of a copy of the whole data and to introducing additional burden in online users on the cloud and storage correctness is to ensure that there is to exists no cheating in cloud server that can be used to pass the audit from TPA without indeed storing cloud user data intact. And privacy preserving is to ensure that there to exist no way for TPA to derive the data content from where the information had collected during the process of Batch auditing and to enable the TPA with the secure and efficient auditing capability to cope with the multiple auditing delegations from possibly a large number of different online users simultaneously. Lightweight to allow the TPA to perform the auditing with minimum communication between the cloud server and online users it shown as a diagrammatic form in below check once.

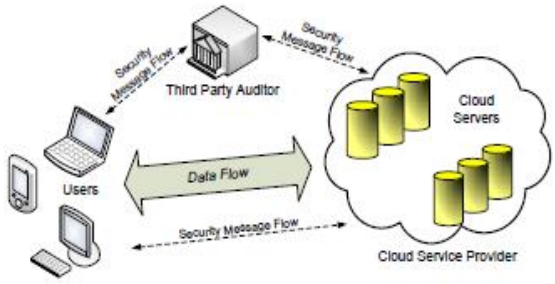

Fig. 1: The architecture of cloud data storage service

Fig. shows the overall process of data transferring and getting the permissions and how to storing in clouds.

[1] In general the user has to store the data in clouds directly but we are allowing another third party to work on it for the security reasons.

[2] Whenever the user want to get the data and to store he can trust on cloud his data should not be corrupt and it's be in safe in Cloud servers

[3] In this process we may stop the attacks from the hackers and in more securable.

[4] Finally, in the case of a service check-in, the cloud server and user may feel burden less of outsourcing data.

MAC-based Solution: We have two possible ways to make use of MAC to authenticate the data. This is a trivial way it's just uploading the data blocks with their MACs to the server and sends the corresponding secret key *sk* to the TPA users. Later, the TPA can randomly retrieve blocks with their MACs and to check the correctness via *sk*. Apart from The high (linear in the sampled data size) communication, for the computation complexities, in the TPA requires the knowledge of the data blocks for verification. The requirement of the data in TPA verification and one may restrict the verification to just consist of equality checking and idea is as follows. Before the data outsourcing in cloud user And chooses *s* random message authentication code keys $\{sk_\tau\}$ $1<=\tau<=s$ precomputes s (deterministic) MACs, $\{MAC_{sk\tau}(F)\}_{1\le\tau\le s}$ for the whole data file F and it publishes these verification metadata in server (the keys and the MACs) to TPA. So the TPA can reveal a secret key sk_τ to the cloud server and asks for a fresh keyed MAC for comparison to each audit. This is privacy-preserving and as long as it is impossible to recover F in a full given $MAC_{sk\tau}(F)$ and sk_τ However it suffers from the following severe drawbacks they are in bellow:

1) How many times a particular data file can be audited is limited by the number of secret keys that it must be fixed a priori. And all possible secret keys are exhausted, so to the user then how to retrieve data in full to re-compute and re-publish as a new MACs to TPA.

2) The TPA has to maintain and update different states between the audits, i.e., keep track on the revealed MAC keys and to Consider that the potentially large number of audit delegations from

Different no of users, maintaining such states for TPA can be a difficult and error prone.

3) This can only support static data, and it cannot be efficient deal with dynamic data at all time. However, it supporting data dynamics is also of critical importance in cloud storage systems. For the reason of clarity, so the main protocol will be presented based on static data of user.

III. Results

In this paper we are provided security to the cloud server storage data users for the providing of this security and response of data we are involved an another third party authenticator for to reduce the burden in cloud server and as well as users also in general we do this process like the data users can store the data directly on cloud in that time cloud may not be responsible for all the data whatever the user stored sometime it may not able to provide the security to the data so to solve this we involved and he has to decrypt the file and store that file in cloud severs and when he storing the data user get an another key from the cloud server in general when user stored the file he have one key and after that when TPA has uploaded the file it generates one more security step the user data and then from the cloud user can get again one more key randomly so whenever the user want to get that file he need to upload all these keys. So here we have two stages of security steps to protect the data whatever user stored in cloud services and then after when user need this data he has to enter through all these two steps then only he can get the file otherwise he cannot get the file and then we can simply identify the user who trying to get the file. It's is very burden less process on cloud server and to user also.

IV. Conclusion

In this application we propose a privacy-preserving public auditing system for secured data in Cloud Computing. And in this we are taking the TPA help to store the user secured data. We are provided two levels of security steps to the user which data users are storing in cloud servers so in this we are used a general masking TPA for the authentication purpose and in this he does not have any knowledge about the data user stored in cloud servers he just only audit the data during the time of data storing in to the cloud servers and the data content stored on the cloud server during the efficient auditing process, which was not only to eliminates the burden of cloud user from the tedious and possibly expensive auditing tasks, but also alleviates the cloud users fear of their outsourced data attach and losing of it. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we are extend that for the further purpose of users and our privacy preserving public auditing was involved into a multi-user setting, where as the TPA can perform the multiple auditing tasks in a batch manner, i.e., similarly to Extensive analysis and to shows that the proposed

schemes are provably secure and highly efficient in cloud servers.

REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud omputing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS /cloud-computing/index.html, 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. onwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"Above the clouds: A berkeley view of cloud computing," University ofCalifornia, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[3] Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at http://status.aws.amazon.com/s3-20080720.html, July 2008.

[4] S. Wilson, "Appengine outage," Online at http://www.cio-weblog.com/ 50226711/appengine outage.php, June 2008.

[5] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Cryptology ePrint Archive, Report 2007/202, 2007, http://eprint.iacr.org/.

[7] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS'09*, Saint Malo, France, Sep. 2009.

[9] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.

[10] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. of Asiacrypt 2008*, vol. 5350, Dec 2008, pp. 90–107.

[11] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 584–597.

[12] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in *Proc. of HotOS'07*. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[13] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/ admnsimp/pl104191.htm, 1996, last access: July 16, 2009.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in *Proc. of IEEE INFOCOM'10*, San Diego, CA, USA, March 2010.

[15] D. Boneh and C. Gentry, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of Eurocrypt 2003, volume 2656 of LNCS*. Springer-Verlag, 2003, pp. 416–432.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," Cryptology ePrint Archive, Report 2009/579, 2009, http://eprint.iacr.org/.

[17] M. Bellare, J. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," in *Proceedings of Eurocrypt 1998, volume 1403 of LNCS*. Springer-Verlag, 1998, pp. 236–250.

[18] C. Schnorr, "Efficient identification and signatures for smart cards," in *Proceedings of Eurocrypt 1989, volume 435 of LNCS*. Springer-Verlag, 1989, pp. 239–252.

[19] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Proceedings of Eurocrypt 1996, volume 1070 of LNCS*. Springer-Verlag, 1996, pp. 387–398.

[20] A. L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in *Proceedings of CT-RSA, volume 5473 of LNCS*. Springer-Verlag, 2009, pp. 309–324.

AUTHOR PROFILE

Ganesh mouli Bandari pursuing M.Tech (IT) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Dr.N.Subhash Chandra, Professor (CSE Department) at Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

V.Krishna, Associate Professor & HOD (IT Department) at Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD