International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Privacy-Preserving Public Auditing for Secure Cloud Storage using ElGamal Public Key Encryption Algorithm

Rahul Vijay Badhe[1], Shriniwas Gadage[2]

[1]PG Student, Department of Computer Engineering, G.H.R.C.E.M., Pune, India

[2]Faculty, Department of Computer Engineering, G.H.R.C.E.M., Pune, India

Abstract: ***The Cloud registering is a most recent engineering which gives different administrations through web. The Cloud server permits client to store their data on a cloud without stressing over accuracy & trustworthiness of data. Cloud data stockpiling has numerous preferences over nearby data stockpiling. Client can transfer their data on cloud and can get to those data at whatever time anyplace without any extra load. The User doesn't need to stress over capacity and support of cloud data. Anyway as data is put away at the remote place how clients will get the affirmation about put away data. Henceforth Cloud data stockpiling ought to have some system which will determine capacity rightness and respectability of data put away on a cloud. The real issue of cloud data stockpiling is security. Numerous specialists have proposed their work or new calculations to accomplish security or to resolution this security issue. In this paper, we propose a safe cloud storage framework supporting protection safeguarding open reviewing. We further augment our result to empower the TPA to perform reviews for numerous clients all the while and effectively. Broad security and execution investigation demonstrate the proposed plans are provably secure and very effective.***

Keywords: Privacy Preserving, Public Auditing, TPA, Security, HLA, HRA.

1. Introduction

Cloud computing is utilizing equipment and programming as figuring assets to give benefit through web. Cloud computing gives different administration models as stage as an services 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) & a lot of people more. Out of this Paas, Saas and Iaas are generally well known. Cloud computing has four models as Public cloud: however which the administration is accessible to all open utilization. Private cloud: Through which administration is accessible to private undertaking or association. Group Cloud: It permits us to impart foundation among different associations through which we can attain security, agreeability and purview. This can be overseen inside or by an outsider and facilitated inside or remotely. Half breed cloud: it is a blend of open and private cloud. Cloud computing has numerous focal points as: we can undoubtedly transfer and download the data put away in the cloud without agonizing over security. We can get to the data from anyplace, at whatever time on interest. Expense is low or pay for every use premise. Fittings and programming assets are effortlessly accessible without area autonomous. The real burden of cloud computing is security.

A. Security Issues:

The security is a real issue in cloud computing. It is a sub space of machine security, system security or else data security. The cloud computing security alludes to an expansive set of approaches, engineering & controls conveyed to secure data, application & the related foundation of cloud computing. Some security and protection issues that need to be viewed as will be as per the following

1) Authentication: Just approved client can get to data in the cloud.
2) Correctness of data: This is the path through which client will get the affirmation that the data put away in the cloud is secure.
3) Availability: The cloud data ought to be effortlessly accessible and open without any load. The client ought to get to the cloud data as though he is getting to nearby data.
4) No storage Overhead and easy maintenance: Client doesn't need to stress over the stockpiling necessity & support of the data on a cloud.
5) No data Leakage: The client data put away on a cloud can got to by just approve the client or holder. So all the substance are available by just approve the client.
6) No Data Loss: Supplier may shroud data misfortune on a cloud for the client to keep up their notoriety. In cloud computing, cloud data stockpiling contains two substances as cloud client and cloud administration supplier cloud server.

Cloud client is an individual who stores extensive measure of data on cloud server which is overseen by the cloud administration supplier. Client can transfer their data on cloud without stressing over capacity and upkeep. A cloud administration supplier will give administrations to cloud client. The significant issue in cloud data stockpiling is to acquire rightness and honesty of data put away on the cloud. Cloud Service Provider (CSP) needs to give some type of component through which client will get the affirmation that cloud data is secure or is put away as it seems to be. No data misfortune or alteration is carried out.

The rightness of data can be abused because of an expansive scope of both inner and outside dangers and CSP may conceal data misfortune or harm from clients to keep up a

notoriety. Significant security issues connected with cloud client and CSP are as per the following:

1) Cloud Service Provider (CSP): Association or undertakings give different administrations to cloud clients. Classifiedness and trustworthiness of cloud data ought to be kept up by CSP. The Provider ought to guarantee that client's data and application are secured on a cloud. CSP may not release the data or else can't adjust or access client's substance. The assailant can log into system correspondence [9].

2) Cloud Server (CS): The cloud server where data being put away and got to by cloud data manager or clients. Data ought not be gotten to by unapproved clients, no data adjustment or no loss of data.

3) Cloud User: Assailants can get to fundamental data like username and secret word [9]. Key administration is major issue in encryption methods. Data element issues need to be considered by CSP. Cloud computing Threads [9] are as per the following:

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

To attain security, we can handover our data to a third outsource party who will define the accuracy and uprightness of the cloud data. Subsequently, new idea touches base as Third gathering examiner (TPA) who will review the client data put away on the cloud, taking into account the client's appeal. For this situation, the Cloud administration supplier doesn't need to stress over the accuracy and honesty of the data. In this method, TPA will review the cloud data to check the honesty or accuracy in two courses as:

1) Download all records and data from the cloud for reviewing. This may incorporate I/O and system transmission cost.
2) Apply evaluating process just for getting to the data yet again for this situation, data misfortune or data harm can't be characterized for unaccessed data. Open review capacity permits client to check respectability of outsource data under diverse framework & security models. We can't attain security as TPA can see the real substance put away on a cloud amid the reviewing stage. TPA itself may release the data put away in the cloud which disregard data security. To dodge this, Encryption method is utilized where data is scrambled before putting away it on the cloud.

2. Related Work

A. MAC Based Solution:

It is utilized to confirm the data. In this, client transfer data pieces and MAC to CS give its mystery key SK to TPA. The TPA will haphazardly recover data pieces & Mac utilizes mystery key to check accuracy of put away data on the cloud. Issues with this framework are recorded underneath as:

- It acquaints extra online trouble with clients because of constrained utilization (i.e. Limited utilization) and stateful check.
- Communication & processing many-sided quality.
- TPA obliges data of data squares for check.
- Limitation on data documents to be reviewed as mystery keys are settled.
- After uses of all conceivable mystery keys, the client needs to download all the data to recomputed MAC & republish it on CS.
- TPA ought to keep up & redesign states for TPA which is extremely troublesome.
- It underpins just for static data not for element data.

B. HLA Based Solution:

It underpins proficient open reviewing without recovering data piece. It is collected and obliged consistent transfer speed. It is conceivable to register a total HLA which verifies a direct mix of the individual data squares.

C. Privacy Preserving Public Auditing Proposed by Cong Wang:

Open examining permits TPA alongside client to check the uprightness of the outsourced data put away on a cloud & Privacy Preserving permits TPA to do inspecting without asking for neighborhood duplicate of the data. Through this plan [1], TPA can review the data and cloud data protection is kept up. It contains 4 calculations as:

1) Keygen: It is a key era calculation utilized by the client to setup the plan.
2) Singen: It is utilized by the client to produce confirmation metadata which may incorporate advanced mark.
3) GenProof: It is utilized by CS to create a confirmation of data stockpiling rightness.
4) Verifyproof: Utilized by TPA to review the evidences It is isolated into two sections as setup stage and review stage.

1) Setup Phase: Open and mystery parameters are introduced by utilizing keygen and data records f are preprocesses by utilizing singen to create check metadata at CS & erase its neighborhood duplicate. In preprocessing client can modify data records F.

2) Audit Phase: TPA issues a review message to CS. The CS will infer a reaction message by executing Genproof. TPA checks the reaction utilizing F and its confirmation metadata. TPA is stateless i.e. no compelling reason to keep up or upgrade the state data of review stage. Open key based homomorphic direct confirmation with irregular veiling system is utilized to attain protection safeguarding open inspecting. TPA checks the trustworthiness of the outsourced data put away on a cloud without getting to genuine substance. Existing exploration work of confirmation of retrievability (Por) [20] or Proofs of Data Possession (PDP) method doesn't consider data security issue. PDP plot initially proposed by Ateniese et al. used to identify substantial sum defilement in outsourced data. It utilizes RSA

based Homomorphic confirmation for examining the cloud data and haphazardly testing a couple of pieces of documents. A Second system proposed by Juels as Proofs of retrievability (Por) permits client to recover records without any data misfortune or debasements. It uses spot checking & blunder remedying codes are utilized to guarantee both "Ownership" and "Retrievability". To attain Zero data protection, specialist [3] proposed Aggregatable Signature Based Broadcast (ASBB). It gives culmination, protection and soundness. It utilizes 3 calculations as Keygen, Gen and Audit.

D. Using Virtual Machine:

Abhishek Mohta proposed Virtual machines which utilize RSA calculation, for customer data/record encryption and decoding [5]. It likewise utilizes SHA 512 calculation which makes message process and check the data uprightness. The Digital mark is utilized as a character measure for customer or data manager. It takes care of the issue of trustworthiness, unapproved access, protection and consistency.

3. Existing System

The cloud data stockpiling administration contains 3 separate substances as cloud client, Third gathering inspector & cloud server/ cloud administration supplier. Cloud client is an individual who stores extensive measure of data or documents on a cloud server. Cloud server is a spot where we are putting away cloud data and that data will be overseen by the cloud administration supplier. Outsider examiners will do the examining on clients demand for capacity rightness and uprightness of data. The proposed framework details that client can get to the data on a cloud as though the neighborhood one without stressing over the respectability of the data.

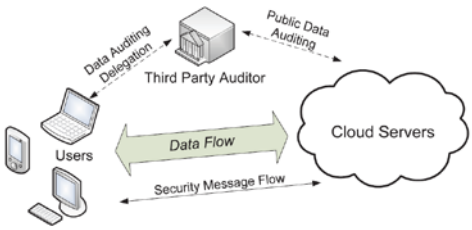


Figure 1: The Architecture of cloud data storage service.

Henceforth, TPA is utilized to check the honesty of data. It upholds security protecting open evaluating. It checks the trustworthiness of the data, stockpiling accuracy. It additionally upholds data motion & bunch inspecting. The significant profits of putting away data on a cloud is the help of load for capacity administration, general data access with area free & evasion of capital consumption on equipment, programming & individual support. In cloud, data is put away in a concentrated structure and dealing with this data and giving security is a troublesome errand. TPA can read the substance of data holder henceforth can adjust. The unwavering quality is expanded as data is taken care of by TPA yet data respectability is not attained. It utilizes encryption system to encode the substance of the document. TPA checks the respectability of the data put away on a cloud however in the event that the TPA itself releases the client's data. Henceforth the new idea comes as reviewing with zero data protection where TPA will review the clients' data without seeing the substance. It utilizes open key based homomorphic direct verification (HLA) [1], [2] which permits TPA to perform inspecting without asking for client data. It decreases correspondence & calculation overhead. In this, HLA with arbitrary veiling convention is utilized which does not permit TPA to learn data content.

A. Goals

- It permits TPA to review clients' data without knowing data content.
- It backings clump evaluating where various client demands for data inspecting will be taken care of all the while.
- It gives security and builds execution through this framework.

B. Design Goals

1) Public audit ability: Permits outsider examiner to check data rightness without getting to neighborhood data.
2) Storage Correctness: The data put away on a cloud is as it. No data alteration is carried out.
3) Privacy preserving: TPA can't read the clients' data amid the evaluating stage.
4) Batch Auditing: Various clients examining solicitation is taken care of all the while.
5) Light Weight: Less correspondence and processing overhead amid the examining stage.

C. Batch Auditing

It additionally backings cluster inspecting through which proficiency is moved forward. It permits TPA to perform various evaluating assignment all the while and it diminishes correspondence and reckoning expense. Through this plan, we can distinguish invalid reaction. It utilizes bilinear mark (BLS proposed by Boneh, Lynn and Shacham) to attain bunch evaluating. Framework execution will be speedier.

D. Data Dynamics

It additionally backs data motion where client can habitually redesign the data put away on a cloud. It backings piece level operation of insertion, cancellation and alteration. Creator of [6] proposed plan which help synchronous open audability and data motion. It utilizes Merkle Hash Tree (MHT) which meets expectations just on scrambled data. It [11] utilizes MHT for piece label confirmation.

4. Proposed System

I am proposing a "Security Preserving Public Auditing System for Data Storage Security" in cloud computing. I will use the Homomorphic Random Authenticator (HRA) by utilizing Elgamal Public Key Encryption Algorithm and arbitrary concealing to ensure that the, TPA would not realize any data about the data substance put away on the

cloud server amid the effective evaluating procedure, which not just disposes of the load of cloud client from the repetitive and potentially extravagant inspecting errand, additionally reduces the clients' apprehension of their outsourced data spillage. Considering TPA might simultaneously handle numerous review sessions from distinctive clients for their outsourced data documents, they further broaden our protection safeguarding open examining convention into a multiuser setting, where the TPA can perform various reviewing assignments in a bunch way for better proficiency. Far reaching investigation demonstrates that their plans are provably secure and very productive. With arbitrary concealing, the TPA probably won't has all the vital data to develop a right gathering of straight mathematical statements and in this way can't determine the client's data content.

• The Third-Party Auditor:
TPA check the respectability of outsourced data and be straightforward. TPA to perform reviews for numerous clients at the same time and effectively. TPA review the outsourced data when required. The TPA, who has aptitude and abilities that clients don't, can occasionally check the trustworthiness of all the data put away in the cloud for the clients, which gives a significantly more less demanding and moderate route for the clients to guarantee their capacity rightness in the cloud. In addition, notwithstanding help clients to assess the danger of their subscribed cloud data benefits, the review result from TPA would likewise be valuable for the cloud administration suppliers to enhance their cloud-based administration stage.

• The ElGamal Public Key Encryption Algorithm:
The security of Elgamal is focused around the discrete logarithm issue. To encode and separately unscramble a message, a discrete force is executed. This operation is efficient to register. An aggressor that looks to unscramble a caught message may attempt to recuperate the private key. To this end a logarithm needs to be registered. No real technique exists for this, given certain prerequisites on the introductory gathering are met. Under these circumstances, the encryption is secure. Today the Elgamal calculation is utilized as a part of numerous cryptographic items. The open-source programming Gnupg utilizes Elgamal as standard for marks. For this product and its issues with Elgamal [10] found in late 2003 we will demonstrate the criticalness of right execution of cryptographic calculations.

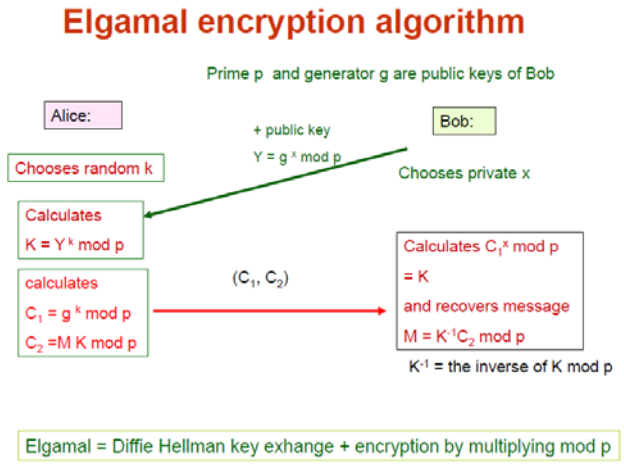
Therefore Elgamal simplified the Diffie-Hellman key trade calculation by presenting an irregular example k. This type is a trade for the private example of the getting substance. Because of this simplification the calculation can be utilized to scramble in one heading, without the need of the second party to take effectively part. The key development here is that the calculation can be utilized for encryption of electronic messages, which are transmitted by the method for open store-and-forward administrations.

The Elgamal Algorithm gives an option to the RSA for open key encryption.
1) Security of the RSA relies on upon the (assumed) trouble of calculating substantial numbers.
2) Security of the Elgamal calculation relies on upon the (assumed) trouble of processing discrete logs in a substantial prime modulus.

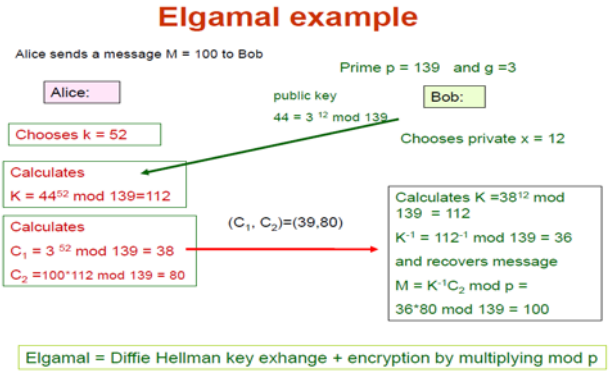
Elgamal has the inconvenience that the ciphertext is twice the length of the plaintext.

It has the playing point the same plaintext gives an alternate ciphertext (with close conviction) each one time it is encrypted.

- The Structure of ElGamal Public Key Encryption Algorithm:



- The Example of ElGamal Public Key Encryption Algorithm:



- Proposed System Architecture:

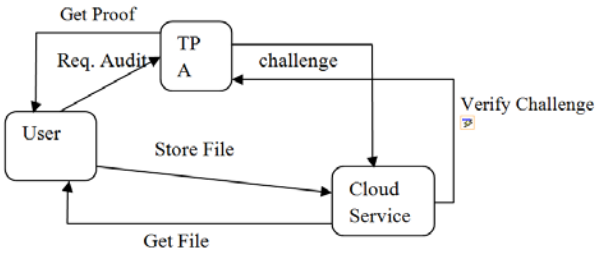


Figure 2: Proposed System Architecture.

User generates Private and public parameters and preprocesses file to create MACs and Store it on cloud Server. He also shares private keys with TPA. TPA creates a Challenge for Cloud Service. Cloud answers the challenge. TPA verifies the answer.

- Proposed System's Real Life Example:

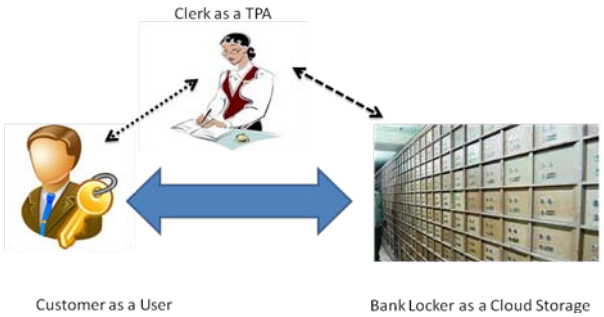


Figure 3: Proposed System's Real Life Example.

5. Conclusion

Along these lines Public Auditing of User Data will be Preserved in cloud computing by use the Homomorphic Random Authenticator (HRA) by utilizing Elgamal Public Key Encryption Algorithm and arbitrary veiling to ensure that the, TPA would not realize any data about the data substance put away on the cloud server amid the proficient examining methodology, which not just takes out the trouble of cloud client from the repetitive and conceivably lavish evaluating errand, additionally eases the client's dread of their outsourced data spillage. Furthermore considering TPA will simultaneously handle various review sessions from distinctive clients for their outsourced data records, they further broaden our protection protecting open reviewing convention into a multiuser setting, where the TPA can perform different inspecting undertakings in a bunch way for better proficiency.

References

[1] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE Trasaction 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 Cloud 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 nad Data Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011.

[8] K Govinda, V. Gurunathprasad and H. sathishkumar, " 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 e print achieve: 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] Lingaraj Dhabale, Priti Pavale, "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] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org.

[20] Juels, B. Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA, USA, 2007. 584-597.

[21] Honywei Li, Yuanshun Dai, Bo Yang. "Identity-Based Cryptography for Cloud Security".