ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(15), DOI: 10.17485/ijst/2016/v9i15/88763, April 2016* ISSN (Online) : 0974-5645

Proxy Key Provisioning Tool (PKPT): A Key Generating Tool for Enhancing Security for Data Integrity Assessment

R. Arunadevi[1*] and K. Nirmala[2]

[1]Manonmaniam Sundaranar University, Tirunelveli - 627012, Tamil Nadu, India; arunaphd2015@gmail.com
[2]Department of Computer Science, Quaid-e-Millath Government College for Women, Chennai – 600002, Tamil Nadu, India; nimimca@yahoo.com

Abstract

Objectives: Proxy Key Provisioning Tool (PKPT) is generated for dynamic key generation for dispatching secured key for protecting them from the attacks when third party assessor assessing data. **Analysis:** In the cloud the privately stored encrypted data retrieved by decoding it using provided key by authenticate users. While the data is stored in various cloud storage by splitting it up into different data chunks then they have to be again integrated using the decoding key that is lively generated by a cryptography algorithm. When the prevailing techniques for regenerating codes that helps in remote private assessing methodologies for ensuring its data integrity that require database holders to be online or appoint any proxy for generating privileged keys for assessors. Some type of privileges like regeneration of authentication in public assessing model only with the help of proxy which can only be semi trusted will help relieve data holder from preserving their data without being online. **Findings:** In our proposed method we deploy an automatic tool termed as Proxy Key Provisioning Tool (PKPT) instead of appointing a proxy server. The key will be generated dynamically and sent to the assessor whenever prompted. This key will have in built timer which will start once the key is dispatched and it have self destruction program once when the set time is over. Thus the key will be protected with strong security so the semi trusting of assessor problem will also be over. Then with the help of this generated key the third party assessor will check for data integrity over the private data from cloud.

Keywords: Cryptography Algorithm, Private Assessing, Proxy Servers, Proxy Key Provisioning Tool (PKPT), Public Assessing, Third Party Assessor

1. Introduction

In cloud storage services increase demand over secured storage service which is outsourced to paradigm of maintenances. Cloud itself provides inbuilt cryptography algorithm for encrypting the data and store it in the privacy preserved area whereas only the data owners with the authenticated decoding key can decode and use the data[1]. Due to severe security threat cloud databases automatically provide data encryption and day by day it updates and enhances its security for data. In some cases cloud providers is forced to release decrypting key that too when it is from high level then they unable to provide security themselves. In that case more than encryption and decryption algorithm cloud storage service needs some enhanced securing technique which will never help anybody other than the legitimate users of that data[2].

Herewith cloud provides splitting up of data into several parts and then they will be encrypted and stored in cloud database. In this case the data owners as well as cloud service providers lose any control with data[3]. When the data is segregated and stored with encrypted cipher text there is no assurance of data availability although there is no guarantee for data integrity[4]. There is a huge

* *Author for correspondence*

risk for data being deleted permanently or corrupted by external data invasion and so many external sources corrupt cloud services abruptly as insecurity. Mandatory method has to be deployed for scrutinizing the data integrity over the cloud and checks their correctness often with secured provision of key to decrypt the data.

Implementation of regenerating codes from the proxy server that is just semi trusted which has only half of the keys and the remaining will be with the assessor itself[5]. This may not be as secured as the data integration process will be scrutinized by the assessor which depends on proxy server for getting the key generation. Almost in all private assessment process only the data owners will be checking for data corrections and they themselves will repair it[6]. Public assessing involves the external assessor and either data owner or the proxy system has to stay online for providing them remaining key as third party cannot have full access towards the data.

In our paper we are going to discuss about the various assess methodologies involved in scrutinizing cloud storage data integrity and its requirement. In next section we discuss how accurately Proxy Key Provisioning Tool (PKPT) is used for integrating and scrutinizing database for its correctness. We also discuss briefly about the self destruction timer coding embedded with the sent key that helps in ensuring security for the key after dispersed. In next section the allocation of reputation scores for assessors and splitting of database send to them for assess is appraised. Then in detail we analyze the pros and cons of working with repairing system for cloud database.

In the review of previous works the data integrity checking and the repairing of cloud storage faults is so much dreadful and costly[7]. The overheads for unlimited and bulk storage in clouds will be outsourced for splitting up and encrypting data and stored in various cloud spaces. Verification of data gathered and correcting them if any faults occurred will be a tedious process which takes much of data owner time and encumber secure database storage[8]. Integrity checking and code generation for assess is a failed model for authenticating external assessors using semi trusted proxy.

As explained by Bo Chen single server regeneration codes repairs process for protecting the data for its security and tries to integrate data. When the paradigm of hosting data services in cloud would make individuals threat to secure key generation. The secret keys would have been generated for authenticating the signature then according to some authors they device an assess scheme for encrypting the methodologies that can protect the data from the external assessor himself. So the linear key generating codes could be efficiently adapted for evaluating the codes based on privacy preserving cloud storage service areas[9].

The complete block regeneration authenticates servers for its getting repaired or some failure in gathering data attempts to the flexible and efficiency oriented proxy servers[10]. There is many kind of regeneration of blocks that might be systematic and regularly archive storage system that could enable network functionality into an order. Many randomized methodologies and techniques so far accomplishing some protection over cloud storage spaces.

Another article appreciates the method of code regeneration for distributed storage and public assessing system that could gather the key again from storage servers where its file is being located[11]. As a prior measure this type of key generation repeatedly store data and their keys in accordance with loss of code problem. The data from various sub servers will be gathered by the regeneration code scheme immediately when it senses the main server faces with data repair. There could be a significant corruption and repairing of data bandwidth for original file could store the cost of repairing file recovers relevant and optimal points for regenerating the feasible files from its corresponding servers[12]. It denotes various parameters that have feasible bandwidth cost that regenerate codes from their storage servers.

2. Private and Public Assess for Cloud Shared Data

In a cloud shared storage services the data that is separated and stored have to be scrutinized for its data integrity and veracity. The genuine data will be authenticated by an external assessor who performs assess for the data that is stored in cloud servers using encryption and data segregation[13]. Data holder who possess massive quantity of data files locate a cloud storage service and have storage in it. The cloud service providers managing the cloud service significantly provide protection to the data like encrypting the information and then splitting it up into chunks of data and store it in diverse areas of cloud storage services.

Assessing protocols are launched thus to gain confidentiality over data vendors as the assessors should

gain self assurance for data not to be leaked anywhere. Whenever any data updated by the data holder then it also should have status of update with the data assessor[14,15]. To secure data from remote checking assesses the protocols will be given to multiple assessors which is stored in various different clouds. This also permits assessor checks for data integrity with which is gathered from all the split up area.

In most of the cloud databases the stored data will undergo assessing for correction checking and assures data integrity. If anything seems to be wrong then the appropriate data will be repaired and replaced in that allotted data space of cloud[16,17]. To evaluate is the main work of an assessor who will usually have half of the key due to security reasons as they cannot be fully relied upon. Thus they undergo periodical assessing and also whenever the user updates or prompts for assessing. That time the user system or the proxy appointed by the user has to be online to issue the next half of the key for the assessor whenever prompted by him.

As depicted in Figure1 the private assessing technique involves single assessor who the data vendor himself use to assess his database for the less amount of data they stored in cloud database. As only the authorized owner is involved there is no problem for security but this can only be available for less data to be stored in a cloud storage spaces[18]. It might not be so complicated while storing and assessing but when any problem occurs and its complicacy increases for the repairing process. When the data owner involved in repairing process then he have to contact the other server having the duplicate copy of his data which can be obtained by providing the key[19]. But it is somewhat tedious and expensive for bulk data involved.

Public assessing came into existence for the purpose of serving huge amount of database stored which cannot be handled solitarily by the owner of data himself. Here assessing of cloud stored database has become public by batch assessing process[20]. To give high protection database will be split up and stored in various cloud with encryption. Data from various cloud databases will be allotted for various different assessors to inspect the integrity of data[21]. As multiple assessors involved for single set of huge database there exists data security for which only one set of data will not help people[22]. So only the part of data will be checked for its integrity by the assessor thus unaware of remaining parts.

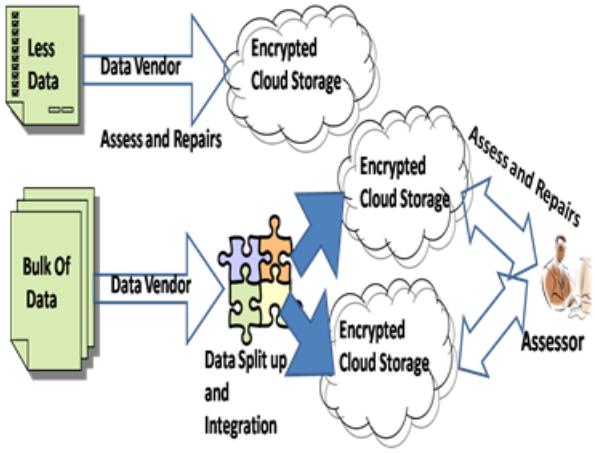

Figure 1. Public and private assessment in cloud storage services.

Many linear equations and combinations help protecting the privacy of data by using batch allotment for assessing the data integrity[23]. This kind of assessing system analyze the data integrity and process data repairing with feasible cost and within stipulated time without having much of the users time. In this method the problem is the data vendor or the proxy system should be online for the entire process of assessing[24]. Whenever the assessor prompts for key the user or proxy system should provide with this is an inconvenient task where there exist many problems like huge waiting time, multiple person involvement and costly, assessing cost is more than storage cost etc. whereas these problems can be conquered by implementing our proposed tool named Proxy Key Provisioning Tool (PKPT) that helps automatic key generation for assessors.

3. Proxy Key Provisioning Tool (PKPT) Implementation

In the process of bulk data storage in cloud database it involves batch assessing data from cloud databases using split up storage. This parameter is implemented for single user storing huge bulk of data by splitting it up and storing it in multiple clouds for which the data vendor holds same type of key generation. Thus a single assessor or multiple assessors depending upon the size of the data indulged. As the cloud stored data will be encrypted the assessor need a decryption key to decipher the cipher text

but the assessor can only be semi trusted for its privacy preserving of entrusted data. So only half the key is given to them the next half will be usually generated by the data vendor or the proxy server appointed by the vendor.

Proxy Key Provisioning Tool (PKPT) facilitates both the user and the assessor by installing it in the data holders system with which the appropriate key will be provided whenever it is prompted by the assessor. Data outsourcing is the tedious and risky task for preserving data security and the data integrity is on heavy risk while storing in the common storage space. Hence this tool automatically generates provisioning key which combines with the key that is with the assessor and decrypt the data. If the data is segregated and stored in various different clouds then that will be decrypted and gathered together to ensure its precision and data integrity. For ideal security the data will be stored in various clouds by split up thus it has to be gathered together for scrutinizing their veracity of data.

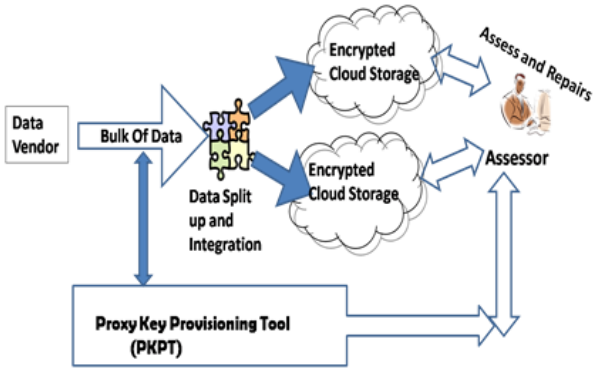

Figure 2. Assessing by obtaining keys from PKPT.

For example, say the vendor protects his data with nine split-ups and stored in various cloud storage services then the assessor will get hold of nine keys to decipher it which is only the half of the code. Full code of key will not be revealed to the assessor thus the remaining code will be stored with the automated PKP Tool. Thus with the prior notification to the data vendor or at the usual periodical checking time the assessor request the user for remaining code for key generation. At that time the PKP Tool installed in the users system will generate the remaining key and send to the assessor. Prior to that PKPT checks for the authenticity of the assessor by checking their validations with its pre stored information about the assessor appointed for assessing the database integrity.

Then it reveals each and every code for generating key each time it is processed then the assessor will combine both the keys that is with him and the obtained key from the user and generates decrypting key. This key reveals the data from the cloud database and the assessor will undergo the process of scrutinizing the data integrity. Then again the data will be encrypted and stored in their appropriate places where it was already. This process involves only the data vendor and the assessor.

When problem occurs during this process then the assessor will handle it as much as he can only when he cannot handle it he handovers to the user. Like when sending keys if any one key is lost or corrupted then the user cannot scrutinize the veracity accurately. Thus he should prompt the user for further key generation even this could have a solution in PKP Tool. With which an extra key will be stored that can be revealed to the assessor only after the user permission is granted. This spare key helps in generating all the other nine keys for further scrutinizing process.

Security assured with these generated keys as any intruder can use it or corrupt it thus an automatic time will be set with the sent key. Each and every key after the assessors request once it sent the timer will be started in it after the fixed time is over the key will be automatically destroyed. So the key cannot be used or acquired by any of the external users or intruders. For time out or for corrupted reasons with which the assessor cannot use that key then he has to again get authentication from the data owner and only after the permission is granted from him the spare key will regenerate all the codes once again.

The assessor once found any problem with data integrity then they use to repair it along with repairing algorithm. They can also regenerate some data and sets them back in their appropriate position. There are many parameters involved in process of repairing and regenerating data from the repairing process or replacing them in their accurate places. Merely this is an outsourced data for which the private cloud protocols supports dynamic data verification and its privacy protection. Data retrieval from the error occurred data is the efficient task encumbered by the assessor which differs from high and less expensive according to the level of error or corruption occurred in the database. This may occur sometimes in case of huge bulk of data storage space in cloud like public environment. Thus if the assessor could not handle this problem by himself then the user have to replace it from their alternate storage thus they should have subsequent alternative for their data to be preserved and stored.

4. Reputation Score Accreditation with Analysis

In case of number of clouds and given high accredited security some data holders appoint more than two assessors for inspecting their data accuracy and data integrity. As data can be stored in split-ups at various clouds they also can be scrutinized separately by various different assessors[25]. Those third party assessors are not even known to each other thus data protection will be very high in this case.

In remote archiving of assessing data checking on-spot and ensuring their correctness generalize the protocols for improvising the variable with private auditing[26]. When multiple assessors involved in integrity scrutinizing process then they all will be categorized with reputation scores by the data vendor. Former to the assessing of main data process all the external assessors will be given some less secured data and according to their efficiency and performance they all will be rated. Everyone will be given reputation score according to which their reliability scores will be accredited in accordance with their performance, efficiency, promptness, evaluation technique and trustworthiness.

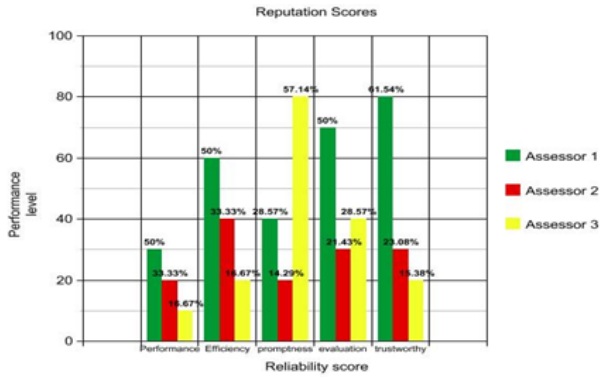

Figure 3. Graph analysis of reliability score report.

According to the Figure 3 each and every assessor will be evaluated and their reputation scores will be accredited. Then according to the scores further data will be given to them for assessing. Assessor with high reputation scores will be given the maximum secure data to be scrutinized and according to the descending scores the data will be provides. The least scorer will be put on hold for alternate purposes. Data provided for assessment to them only during emergency or critical period where none of the high scorers is available for scrutinizing data integrity. Thus cloud storage database acquires high security in multiple ways.

5. Conclusion

In our proposed paper we implement Proxy Key Provisioning Tool (PKPT) which generates code for key when an assessor is scrutinizing the data. As it is implemented in the user system its security is assured and to protect the key generation algorithm from the intruders multiple security procedures is provided to them. Various assessors involved in assessing data from various cloud storage spaces for the single data owner possessing single decrypting key facilitates the accuracy and data integrity more than its assurance of data security. This mainly eliminates the time and cost expenditure of the data vendor always being online and data outsourcing expenses. Reputation score accreditation to various integrity assessors helps analyzing and preferring of best assessor for our valuable data stored in public storage space. The self destruction timer present in PKPT guarantees the second usage of key by any intruders. Cloud storage services can be more available with highly secured environment and data assessors provide high degree of certain data integrity.

6. References

1. Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: A Berkeley view of cloud computing. Dept Electrical Eng and Comput Sciences, University of California, Berkeley, Rep. UCB/EECS. 2009; 28:1–42.
2. Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, ACM; New York, NY, USA. 2007. p. 598–609.
3. Juels A, Kaliski BS, Jr. Pors: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM; 2007. p. 584–97.
4. Curtmola R, Khan O, Burns R, Ateniese G. Mr-pdp: Multiplereplica provable data possession. The 28th International Conference on Distributed Computing Systems. 2008. ICDCS'08, IEEE; Beijing. 2008 Jun 17-20. p. 411–20.
5. Bowers KD, Juels A, Oprea A. HAIL: A High-Availability and Integrity Layer for cloud storage. Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM; 2009. p. 187–98.

6. He J, Zhang Y, Huang G, Shi Y, Cao J. Distributed data possession checking for securing multiple replicas in geographically dispersed clouds. Journal of Computer and System Sciences. 2012 Sept; 78(5):1345–58.
7. B. Chen, R. Curtmola, G. Ateniese, R. Burns. Remote data checking for network coding-based distributed storage systems. Proceedings of the 2010 ACM workshop on Cloud Computing Security Workshop. ACM; 2010. p. 31–42.
8. Chen H, Lee P. Enabling data integrity protection in regenerating coding-based cloud storage: Theory and implementation. IEEE Transactions on Parallel and Distributed Systems. 2014 Feb: 25(2):407–16.
9. Yang K, Jia X. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Transactions on Parallel and Distributed Systems. 2013 Sep; 24(9):1717–26.
10. Zhu Y, Hu H, Ahn GJ, Yu M. Cooperative provable data possession for integrity verification in multicloud storage. IEEE Transactions on Parallel and Distributed Systems. 2012 Dec; 23(12):2231–44.
11. Dimakis AG, Ramchandran K, Wu Y, Suh C. A survey on network codes for distributed storage. Proceedings of the IEEE. 2011 Mar; 99(3):476–89.
12. Shacham H, Waters B. Compact proofs of retrievability. Advances in Cryptology -ASIACRYPT 2008. Springer. 2008; 5350:90–107.
13. Hu Y, Chen HC, Lee PP, Tang Y. Nccloud: Applying network coding for the storage repair in a cloud-of-clouds. USENIX FAST; 2012.
14. Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. INFOCOM, 2010 Proceedings IEEE; San Diego, CA. 2010 Mar 14-19. p. 1–9.
15. Wang C, Chow SS, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 2013 Feb; 62(2):362–75.
16. Wang C, Wang Q, Ren K, Lou W. Towards secure and dependable storage services in cloud computing. IEEE Transactions on Service Computing. 2012 Apr-Jun; 5(2):220–32.
17. Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing. Journal of Cryptology. 2004 Sep; 17:(4):297–319.
18. Dimakis AG, Godfrey PB, Wu Y, Wainwright MJ, Ramchandran K. Network coding for distributed storage systems. IEEE Transactions on Information Theory. 2010 Sep; 56(9):4539–51.
19. Ho T, Medard M, Koetter R, Karger DR, Effros M, Shi J, Leong B. A random linear network coding approach to multicast. IEEE Transactions on Information Theory. 2006 Oct; 52(10):4413–30.
20. Boneh D, Freeman D, Katz J, Waters B. Signing a linear subspace: Signature schemes for network coding. Public Key Cryptography - PKC 2009. Springer. 2009; 5443:68–87.
21. Vijayan K, Raaza A. A novel cluster arrangement energy efficient routing protocol for Wireless Sensor Networks. Indian Journal of Science and Technology. 2016 Jan; 9(2):1–9. Doi no: 10.17485/ijst/2016/v9i2/79073.
22. Sathick KJ, Jaya A. Natural language to SQL generation for semantic knowledge extraction in social web sources. Indian Journal of Science and Technology. 2015 Jan; 8(1):1–10. Doi no: 10.17485/ijst/2015/v8i1/54123.
23. Vigneshwari S, Aramudhan M. Social information retrieval based on semantic annotation and hashing upon the multiple ontologies. Indian Journal of Science and Technology. 2015 Jan; 8(2):103–7. Doi no: 10.17485/ijst/2015/v8i2/57771.
24. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3):216–21. Doi no: 10.17485/ijst/2015/v8i3/59585.
25. Ramesh N, Andrews J. Personalized search engine using social networking activity. Indian Journal of Science and Technology. 2015 Feb; 8(4):301–6. Doi no:10.17485/ijst/2015/v8i4/60376.
26. Durairaj M, Manimaran A. A study on security issues in cloud based E-Learning. Indian Journal of Science and Technology. 2015 Apr; 8(8):757–65. Doi no: 10.17485/ijst/2015/v8i8/69307.