ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 04, pp.29487-29489, April, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

SECURE SHARING IN CLOUD USING REGENERATED CODE

***Pritha, K. and Nivethitha, M.**

Department of CSE, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India

ARTICLE INFO

Article History:
Received 15th January, 2016
Received in revised form
20th February, 2016
Accepted 24th March, 2016
Published online 26th April, 2016

Key words:

TPA,Group Admin,
Key Generation,
Authentication,
Revocation.

ABSTRACT

Cloud Computing is a service that allows users to store data on offsite storage system managed by third-party and is accessible by a web service API. Data access control is an effective way to ensure the data security in the cloud. The Protection of data integrity and privacy has become one of the issue in cloud computing. The Private auditing technique is achieved by the emergence of the Regenerating code. Regenerating code provide lower bandwidth and fault tolerance. This method requires data owners to stay online and handle auditing. In the proposed paper, we present a public auditing scheme for the regenerating-code based cloud storage. This method solves the regeneration problem in the absence of data owners. The users ask the Third Party Auditor (TPA) to check the integrity of the data. Moreover to preserve data privacy, the data's are encrypted using AES algorithm. Thus our scheme is highly secure and can be feasibly integrated into the regenerating code based cloud storage. The MD5 technique is efficiently used in order to protect the data.

Citation: Pritha, K. and Nivethitha, M. 2016. "Secure sharing in cloud using regenerated code", *International Journal of Current Research*, 8, (04), 29487-29489.

INTRODUCTION

Cloud Computing is used to manipulate, configure and access the hardware and software resources remotely. It provides storing data online, infrastructure and application. The term Cloud refers to Network or Internet. It provides on-demand self-service. The cloud service provider are not used to access the resource. Cloud computing provides a shared pool of resources including data storage space, network, computer processing power and specialized user application. The security and privacy is the biggest problem in cloud computing. Any sign of security breach leads to the loss of data. In this paper, we aim at maintaining the integrity of the data by regenerating the code. The cloud data storage is classified as three basic entities. Cloud user is a person who stores data on a cloud server. Cloud server is a place where we are storing large cloud data and that are managed by cloud service provider. The auditing on users request for storage integrity and correctness is done by the Third party auditor. The security and trust is provided by TPA. TPA should also ensure that there is no problem for data owners. It should not allow any malicious attack or unauthorized access within the cloud.

****Corresponding author: Pritha, K.***
Department of CSE, Kumaraguru college of Technology, Coimbatore, Tamil Nadu, India.

This technique guarantees good performance of audit services and allows maximum access transparency to the data owners. This paper implements secure dynamic auditing protocol.

Literature Survey

Provable Data Possession at Untrusted Source

A client or user will store the data in the server and there is a possibility of retrieving the original data from the server by an untrusted person. Provable Data Possession is a model that helps in verifying that the data stored in the server is original and is not duplicated or retrieved. This model helps in supporting the large data set in widely distributed storage system. By this model we can reduce the I/O cost. It focuses on the problem of verifying if the untrusted user acts maliciously. The assurance of data possession is not confirmed because no security proof is available for this scheme.

PORs: Proofs of Reterivability for large files

The Proofs of Retrievability is the technique where a user is provided a reliable proof to retrieve the target data. This model enables a back-service to provide the proof. It can be considered as a cryptographic Proof of Knowledge, and they are designed to handle large files. POR is efficient enough to provide regular checks for file retrievability. It ensures the

privacy and integrity of files they retrieve. A drawback of this model is that the preprocessing / encoding of File is required prior to storage with the prover. This model imposes some computational overhead. POR only aims at detection of file corruption or loss, and not prevention of files.

Existing System

Numerous methods using attribute based encryption have been proposed to protect the outsourced data from malicious users. A multi-owner data sharing scheme was put forward for dynamic groups in the cloud, so that any users in the group can access and utilize the data anonymously without the knowledge of the data owner. One solution to achieve secure sharing in cloud is that data owner can encrypt his data before storing onto the cloud and hence the data remain theoretically secure against Cloud provider and malicious users. If the data owner wishes to share his data to the group he sends the key used for encryption to the members of the group. The members in the group can use the key to decrypt the data. Since the cloud is not in the trusted domain with every user in the group, sharing of the data owner's private key to all the users in the group may significantly lead to security issue. However, the main issue with this technique is that it makes too much burden to the data owner when it concerns with user revocation. If the data owner revokes any member from group, the data owner should re-encrypt the data and share the new key to the remaining members of the group, rendering the revoked member's key useless. A number of security issues were labeled in the preceding works. Yet a user's privacy is revealed by access request itself as a result of requesting data from the user has not been studied. Hence we introduce regenerating scheme to solve the burden of the data owners and invoke data access control to ensure the privacy of the user's data.

Proposed System

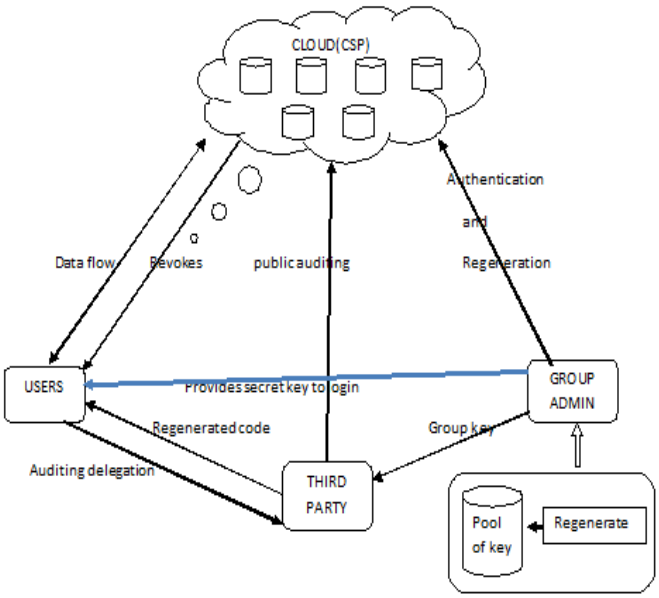
System Model

The cloud storage system model consists of 4 different entities. They are user, group admin, Third party authenticator (TPA), Cloud Service Provider (CSP).The user can store, view and download files from the cloud. The group admin provides a secret key to the user to login into the cloud and regenerates the group key. TPA is responsible for public audit of data and provides group key to the user. CSP provide cloud services, storage and creates a group *Formatting.*

Proposal

In the proposed system the workflow takes place as follow. The users are registered by giving their basic credentials. Users are allowed to select a group in which they has to join. The groups are created and monitored by the group admin. The group admin will provide a key to the user to make further login into the cloud. This key provides an authentication to user login. Once the user login into the cloud, he/she can upload or download the file from the cloud in a secured way. The uploaded user files are encrypted using more powerful AES algorithm and stored in the cloud. If a user want to access the uploaded file of other user he/she should make a request to respective data owner. It is the data owner's privacy whether to accept or deny the request of the requestor. Once the data owner responses to the request, TPA provides the group key to the accepted user. The user can use the key provided by TPA to download the particular file. The group admin can only regenerate the group key and cannot view, use or share the group key to malicious users. The group key is known only for the TPA who is considered to be trustable and revokes user from the cloud if he is found to act malicious. The regeneration of code is done by the MD5 technique. If the user uses the provided key to download a file other than the requested file, the user is added to the revocation list. The TPA revokes the user from the cloud. Once the user is revoked he/she is not allowed to enter into the cloud.

Proposed System Model



Thus with the projected approach, data's are shared effectively among the many teams in cloud. It supports economical user revocation and new user connection. Then, we tend to create a good information access management theme for multi-group cloud storage systems. Considering that the information owner cannot continually keep on-line in apply, so as to stay the storage accessible and verifiable once a malicious corruption, cluster admin act as proxy to handle the reparation of the coded blocks and authenticators. The revocable multi-authority may be a promising technique. This approach greatly reduces the employment on the storage servers. The projected theme is extremely economical and may be feasibly integrated into a regenerating-code-based cloud storage system.

***D.* Algorithm**

AES encryption algorithm is used to encrypt and decrypt the text. The features of AES are as follows:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys

- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. AES encryption comprises four sub-process. The data's are encrypted using these sub-process. They are Byte Substitution, Shift rows, Mix columns, Add round key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. Various researchers have published attacks against reduced-round versions of the Advanced Encryption Standard, and a research paper published in 2011 demonstrated that using a technique called a biclique attack could recover AES keys faster than a brute-force attack by a factor of between three and five, depending on the cipher version. Even this attack, though, does not threaten the practical use of AES due to its high computational complexity.

The MD5 message-digest rule may be a wide used science hash perform manufacturing a 128-bit (16-byte) hash price, generally expressed in text format as a 32-digit hex range. MD5 has been utilized in a very wide selection of science applications and is additionally unremarkably accustomed verify knowledge integrity. MD5 may be a unidirectional function; it's neither cryptography nor secret writing. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is choppy into chunks of 512-bit blocks (sixteen 32-bit words); the message is cushioned in order that its length is partible by 512. The artefact works as follows: initial one bit, 1, is appended to the tip of the message. This is often followed by as several zeros as square measure needed to bring the length of the message up to sixty four bits less than a multiple of 512. The remaining bits square measure crammed up with sixty four bits representing the length of the first message, modulo 264.
The MD5 rule is nominal for messages consisting of any range of bits; it's not restricted to multiples of eight bit (octets, bytes) as shown within the examples higher than. Some MD5 implementations like md5sum may be restricted to octets, or they could not support streaming for messages of Associate in Nursing at the start undetermined length.

Conclusion

Thus with the proposed approach, data's are shared effectively among the several groups in cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. It supports efficient user revocation and new user joining. Then, we constructed an effective data access control scheme for multi-group cloud storage systems. This approach greatly reduces the workload on the storage servers. The proposed scheme is highly efficient and can be feasibly integrated into a regenerating-code-based cloud storage system.

REFERENCES

Ateniese, G. *et al*. 2007. "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York,NY,USA, pp. 598–609.

Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud".

He, J., Y. Zhang, G. Huang, Y. Shi, and J. Cao, 2012. "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," *J. Comput. Syst. Sci.*, vol. 78, no. 5, pp. 1345–1358.

Jahid, S., P. Mittal, and N. Borisov, 2011. ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.R. Nicole, "Title of paper with only first word capitalized*," J. Name Stand. Abbrev*., in press.

Li, J., X. Chen, M. Li, J. Li, P. Lee, and W. Lou, 2014. "Secure regeneration with efficient and reliable convergent key management," in IEEE Transactions on Parallel and Distributed Systems, pp. vol. 25(6), include Networking, Cloud Computing, and Data Mining. pp. 1615–1625.

Li, M., S. Yu, Y. Zheng, K. Ren, and W. Lou, 2013. ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan.

Stanek, J., A. Sorniotti, E. Androulaki, and L. Kencl, 2013. "A secure data regeneration scheme for cloud storage," in Technical Report.

Yang, K. and X. Jia, 2013. "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep.

****