International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Public Auditing for Regenerating Code Based Cloud Storage

Jyoti Mahajan

Student Department of Information Technology,
Amrutvahini College of Engineering, Sangamner
Maharashtra, India

Abstract— *To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation be-comes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, a proxy server is introduced, which is given privilege to regenerate the authenticators, into the traditional public auditing system model. The scheme can completely release data owners from online burden.*

Keyword: Semi-Trusted Proxy, Authenticators, Third Party Auditor

1. Introduction

CLOUD storage is now gaining popularity because it provides flexible, on-demand data outsourcing service with appealing benefits: relief of the burden for storage management, universal data access with location independence and avoidance of capital expenditure on hardware, software and personal maintenances, etc., [1]. Nevertheless, this new paradigm of data hosting service also brings new security threats toward users data, thus making individuals or enterprisers still feel hesitant.

CLOUD storage is now gaining popularity because it provides flexible, on-demand data outsourcing service with appealing benefits: relief of the burden for storage management, universal data access with location independence and avoidance of capital expenditure on hardware, software and personal maintenances, etc., [1]. Nevertheless, this new paradigm of data hosting service also brings new security threats toward users data, thus making individuals or enterprisers still feel hesitant.

It is noted that data owners lose ultimate control over the fate of their outsourced data; thus, the correctness, availability and integrity of the data are being put at risk. On the one hand, the cloud service is usually faced with a broad range of internal/external adversaries, who would maliciously delete or corrupt users' data; on the other hand, the cloud service providers may act dishonestly, attempting to hide data loss or corruption and claiming that the les are still correctly stored in the cloud for reputation or monetary reasons.

2. PROBLEM STATEMENT

The Problem is to that users may not want to go through the complexity in verifying and reparation of data at faulty server. The auditing schemes in [2], [3] imply the problem that users need to always stay online for the owner, which may impede its adoption in practice, especially for long-term archival storage. Also the owner may not be technological efficient and can detect, locate the faulty server. Both the factors can make owner to go for appointing the support team which then look after the data stored in the cloud. Hence the maintenance charges increases. Again adoption of cloud seems to be an expensive option.

3. LITERATURE SURVEY

The term cloud storage means storing public/private data of the owner in the cloud. This technique has gained popularity as it provides following benefits:-

1) Relief from Burden for Storage Management.
2) Universal data access with location independence.
3) Avoidance of capital expenditure on H/W, S/W and personal maintenance.

Since the data owner outsource its data he/she loses complete control on the data .The chance it gets corrupted is high as the malicious user are always finding the new ways to hack and destroy the data stored at data center. Thus, the correctness, availability and integrity of the data are being put at risk. On the other hand, the cloud service providers may act dishonestly, attempting to hide data loss or corruption and claiming that the les are still correctly stored in the cloud for reputation or monetary reasons giving false impression to the data owner.

Therefore data owner has now started relying on the third party which uses a protocol to perform periodical verifications of their outsourced data to ensure that the cloud indeed maintains their data correctly.

But gain considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing and reparation in the cloud can be formidable and expensive for the users .The overhead of using cloud storage should be minimized as much as possible such that a user does not need to perform too many operations to their outsourced data (in additional to retrieving it) .Reiterating the fact that user do not want to go through the complexity in verifying and reparation. And want to always stay online.

To fully ensure the data integrity and save the users' computation resources as well as online burden, a public auditing scheme is proposed for the regenerating-code-based cloud storage, in which the integrity checking and regeneration (of failed data blocks and authenticators) are implemented by a third party auditor and a semi-trusted proxy separately on behalf of the data owner.

4. EXISTING SYSTEM

At present data owner relies on third party auditor which performs periodical verification on the data outsourced by them. The third party performs check and sends alarm signal to the data owner whenever it locate the faulty server .However when some problem is identified it mandates the owner to stay online when problem occurs .And if the owner is technologically deficient it requires full staff to stay online to solve the problem. Hence overhead to stay online increases. This may impede its adoption in practice, especially for long-term archival storage.
The diagram representing existing system:-

Fig 1.0 Existing Auditing Scheme

5. PROPOSED SYSTEM

To fully ensure the data integrity and save the users' computation resources as well as online burden, we propose a public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration (of failed data blocks and authenticators) are implemented by a third party auditor and a semi-trusted proxy separately on behalf of the data owner.
The implementation system model for the above proposed scheme can be found below:-

1) **Data Owner:-** Who owns large amounts of data in cloud.

2) **The Cloud:-** Which are managed by the cloud service provider, provide storage service and have signi cant computational resources.

3) **The TPA (Third Party auditor) :-**Who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud.

4) **A Proxy Agent:-** Who is semi-trusted and acts on behalf of the data owner to re-generate authenticators and data blocks on the failed servers during the repair procedure.

The diagram of new proposed system is:-

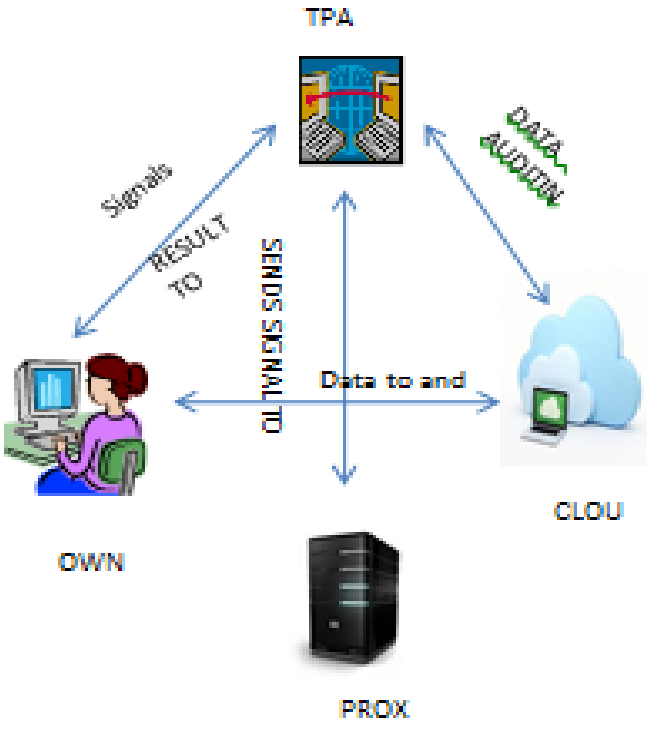

Fig 1.1 Propsed Auditing System

The proposed system will work as follows:-

The user share public key with the TPA and generate partial private keys which is shared by the proxy server so that it can pose as owner in case of faulty server is located.
The owner periodically sends the request to TPA to perform the audit.

If TPA finds any fault then a signal is send to owner and proxy server. The proxy server then comes into action and locate the faulty server, repairs it with the help of partial private keys shared by the owner to the proxy server.
The proxy server regenerates the code and then sends an acknowledgement to the owner.
Hence it eliminates the problem of owner to stay online which is the key point to be handled in this paper.

6. ALGORITHMS AND CLASSES

The paper uses Diffie-Hellman Algorithm to generate keys and get the shared keys[4]:-

Supposing there are two participants of the exchange (let's call them Alice and Bob, as it is traditionally established in cryptography). Both of them know two numbers P and G. These numbers are not secret and can be known to anyone. The goal of Alice and Bob is to obtain the shared secret key to help them to exchange messages in future.

For this, they generate two big random numbers (so called private keys):

Alice - number Xa,
Bob –number Xb.
After this, Alice computes the value of the public key:

Ya = (G^Xa) mod P and sends it to Bob.

In his turn, Bob computes the value of his public key:
Yb = (G^Xb) mod P

And sends it to Alice.

At the second stage, on the basis of her private key and the public key, received from Bob, Alice computes the value
Ka =(Yb^Xa) mod P

Similarly, Bob computes the value
Kb = (Ya^Xb) mod P

Numbers Ka and Kb are equal

Ka = (Yb^Xa) mod P = (((G^Xb) mod P) ^Xa) mod P = (G^XaXb) mod P = (((G^Xa) mod P) ^Xb) mod P = (Ya^Xb) mod P = Kb
and they can be used as the secret key by Alice and Bob.

This algorithm is used to generate and share keys. This algorithm is technically known as a *key-agreement algorithm*. It cannot be used for encryption, but can be used to allow two parties to derive a secret key by sharing information over a public channel. This key can then be used for private key encryption.

The Java inbuilt Cipher class manipulates public key algorithms using keys produced by the KeyPairGenerator class. Thus classes used for public and private keys generation are:-
Cipher
KeyPairGenerator

7. Discussion

The solution proposed in the paper can help in the scenario below:-

Let's say a startup name ABC has just established and has outsourced its data to cloud as it cannot afford to have the entire infrastructure for storage and staff for maintenance of data.

The people cannot stay 24*7 online .Hence it has also outsourced the auditing and repairing of data to the semi trusted third party.

So when owner initiates AUDIT by giving signal to TPA, TPA performs audit and if find any faulty server then instead signaling owner it signals Proxy, thus reducing the overhead of owner to stay online.
The proposed scheme can reduce the time and money spent on the company's functioning.

8. CONCLUSION

In this paper, a public auditing scheme is proposed for the regenerating-code-based cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking. Considering that the data owner cannot always stay online in practice, in order to keep the storage available and verifiable after a malicious corruption, we introduce a semi-trusted proxy into the system model and provide a privilege for the proxy to handle the reparation of the coded blocks.

Acknowledgment

As wise person said about the nobility of the teaching profession, Catch a fish and you feed a man his dinner, but teach a man how to catch a fish, and you feed him for life.

In this context, I would like to thank our helpful project guide Prof. Borkar B.S who had been an incessant source of inspiration and help. Not only did he inspire me to undertake this assignments, he also advise me throughout its course and help me during my times of trouble. I would like to thank H.O.D. of Department of Information Technology Dr. GUNJAL B.L. for motivating me.

Also, I would like to thank other members of Information Technology department who helped me to handle this

assignment efficiently, and who were always ready to help us during times of need.

References

[1] A. Fox, R. Gri th, A. Joseph, R. Katz, A. Konwinski, G. Lee,D. Patterson, A. Rabkin, and I. Stoica, \Above the clouds: A berkeley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences,University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.

[2] H. Chen and P. Lee, \Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," Parallel and Distributed Sys-tems, IEEE Transactions on, vol. 25, no. 2, pp. 407{416,Feb 2014.}

[3] K. Yang and X. Jia, \An e cient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717{1726, 2013.} https://simple.wikipedia.org/wiki/Diffie-Hellman_key_exchange