**International Journal of Technology in Computer Science & Engineering**
ISSN 2349-1582
Volume 4, No 1, March 2017 

# DYNAMIC KEY AND AUDIT SERVICES FOR OUTSOURCED BIG DATA STORAGES

R. Jefia Wilson
PG student, Department of CSE
Ponjesly College of Engineering, Nagercoil
jefiacse@gmail.com

C.Felsy
Assistant Professor,Department of CSE
Ponjesly College of Engineering, Nagercoil
felsyjohn_13@yahoo.co.in

**Abstract:** Key-exposure resistance is an important problem in cyber defense. In the cloud storage auditing the key exposure problem was well analyzed and studied. In the existing solution the client will be updating the secret keys in every period of time so it is very difficult for the client particularly those who are in limited computation resources. In the paper, we focus on how key updates are transparent to the client and propose a new concept called cloud storage auditing with verifiable outsourcing of key updates. Key updates can be safely outsourced to some authorized party and thus the key update work burden to the client will be reduced. In this we leverage the third-party auditor in many existing public auditing designs, let's play the role of authorized party and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. In this design, TPA only needs to hold an encrypted version of the client's secret key while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by the TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. The security proof and the performance simulation show that our detailed design instantiations are secure and efficient.

## 1 Introduction

Cloud computing technology is becoming more and more popular now a days. It can provide users with unlimited computing resource. people can outsource time consuming computation workloads to cloud without spending the extra capital on maintaining hardware and software. In recent years, outsourcing computation has attracted much attention and been researched widely.[6] It has been considered in many applications including scientific computations linear algebraic computations linear programming computations and modular exponentiation computations etc. Besides, cloud computing can also provide users with seemingly unlimited storage resource.[7] Cloud storage is universally viewed as one of the most important services of cloud computing. Although cloud storage provides great benefit to users, it brings new security challenging problems. One important security problem is how to efficiently check the integrity of the data stored in cloud.[2] In recent years, many auditing protocols for cloud storage have been proposed to deal with this problem. These protocols focus on different aspects of cloud storage auditing such as the high efficiency the privacy protection of data the privacy protection of identities dynamic data operations the data sharing etc. The key exposure problem, as another important problem in cloud storage auditing, has been considered recently. The problem itself is non-trivial by nature. Once the client's secret key for storage auditing.

## 2 Related Work

***Outsourcing Computation:*** Time-consuming computations have become a hot topic in the research of the theoretical computer science in the recent two decades. Outsourcing computation has been considered in many application domains [4].A new paradigm called cloud storage auditing system is proposed. In this new technique the key client operation is not performed by the client. The key update operation is performed by the authorized party. The authorized party holds the encrypted secret key of the client for client for cloud storage auditing.[8] The client downloads the encrypted secret key from the authorized party and decrypt it only when the client need to upload any new files to cloud. The client needs to check the validity of the encrypted secret key. The secret keys for cloud storage auditing are updated periodically.[4] As a result, any dishonest behaviors, such as deleting or modifying the client's data previously stored in cloud, can all be detected, even if the cloud gets the client's current secret key for cloud storage auditing. However, the client needs to update his secret key in each time period. Existing solutions all require the client to update the secret keys in every time period which may inevitably bring in new local burdens to the client especially those with limited computation resources. The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed that is the client can upload the growing files to cloud in different time points. The cloud stores the client's files and provides download service for the client. Important security problem is how to efficiently check the integrity of the data stored in storage area. With limited computation resources the users might not like doing such extra computations by themselves in each time period.

## 3 Proposed System

TPA only needs to hold an encrypted version of the client's secret key while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by the TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. The definition and the security model of this paradigm. The security proof and the performance simulation show that our detailed design instantiations are secure and efficient.

### 3.1 Data Producer And Retriever

The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed that is the client can upload the growing files to cloud in different time points. The cloud stores the client's files and provides download service for the client.

### .3.2 Figures

Figures should be drawn in word or in any other word editors. Copying and pasting of graphs and figures are not allowed. Graphs can be drawn in any latest graph editors or with excel. Low quality graphs and figures should not be submitted.

#### *3.2.1 Figures details*

Please check that the lines in line drawings are not interrupted and have a constant width. Grids and details within the figures must be clearly legible and may not be written one on top of the other. Line drawings should have a resolution of at least 800 dpi (preferably 1200 dpi). The lettering in figures should have a height of 2 mm (10-point type). Figures should be numbered and should have a caption which should always be positioned *under* the figures, in contrast to the caption belonging to a table, which should always appear *above* the table. Please center the

captions between the margins and set them in 9-point type (Fig. 1 shows an example). The distance between text and figure should be about 8 mm, the distance between figure and caption about 6 mm.

To ensure that the reproduction of your illustrations is of a reasonable quality, we advise against the use of shading. The contrast should be as pronounced as possible.

If screenshots are necessary, please make sure that you are happy with the print quality before you send the files.

*Remark 1.* In the printed volumes, illustrations are generally black and white (halftones), and only in exceptional cases, and if the author is prepared to cover the extra costs involved, are colored pictures accepted. Colored pictures are welcome in the electronic version free of charge. If you send colored figures that are to be printed in black and white, please make sure that they really are legible in black and white. Some colors show up very poorly when printed in black and white. An example graph is given.

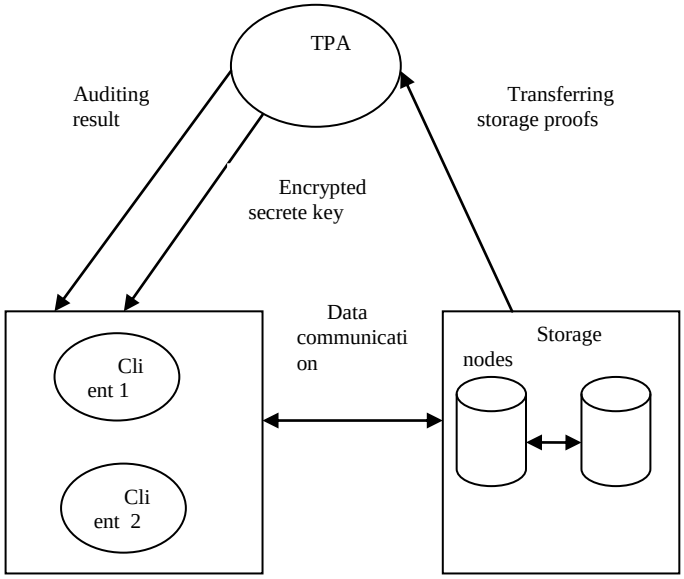


**Fig.:** Architecture Diagram

### 3.2 Third Party Auditor

The TPA plays two important roles:

- The first is to audit the data files stored in cloud for the client.
- The second is to update the encrypted secret keys of the client in each time period.

The TPA can be considered as a party with powerful computational capability or a service in another independent cloud.

### 3.3 Key Updates

The TPA updates the encrypted client's secret key for cloud storage auditing according to the next time period. But the public key keeps unchanged in the whole time periods. The client sends the key requirement to the TPA only when he wants to upload new files to cloud. And then the TPA sends the encrypted secret key to the client. After that, the client decrypts it to get his real secret key, generates authenticators for files, and uploads these files along with authenticators to cloud.

## 4 Conclusion

Key updates for cloud storage auditing with key-exposure resilience. We propose the first cloud storage auditing protocol with verifiable outsourcing of key updates. In this protocol, key updates are outsourced to the TPA and are transparent for the client. The TPA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. Thus the security performance is high.

## 5 References

1. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E.E.Spafford, "Secure outsourcing of scientific computations," Adv. Comput., vol. 54, pp. 215–272, 2008.
2.G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur.Privacy Commun.Netw., 2008, Art. ID 9.
3.G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf of. Comput. Commun.Secur., 2007, pp. 598–600.
4.D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing algebraic computations," in Proc. 6th Annu. Conf. Privacy, Secur.200
5. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular xponentiations," in Proc. 17th Eur. Symp.Res.Comput.Secur.,2012,pp.541–556.
6.C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010 Trust, 2008, pp. 240–245.
7.G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130–139,Mar. 2016.
8.J. Yu, F. Kong, X. Cheng, R. Hao, and G. Li, "One forward-secure signature scheme using bilinear maps and its applications," Inf. Sci.,vol. 279, pp. 60–76, Sep. 2014.
9.J. Yu, R. Hao, H. Zhao, M. Shu, and J. Fan, "IRIBE: Intrusion resilient identity-based encryption," *Inf. Sci.*, vol. 329, pp. 90–104,Feb. 2016