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

International Journal of Current Research
Vol. 7, Issue, 05, pp.16008-16010, May, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

ENABLING AND ENHANCING PUBLIC VERIFIABILITY OF CLOUD DATA USING THIRD PARTY AUDITING

***, [1]Nikhitha K. Nair and [2]Navin, K. S.**

[1]Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram-695543
[2]L.B.S. College of Engineering, Poojapura, Thiruvananthapuram- 695012

ARTICLE INFO

Article History:
Received 20th February, 2015
Received in revised form
15th March, 2015
Accepted 19th April, 2015
Published online 31st May, 2015

Key words:

Cloud computing,
Auditing,
Dual encryption,
AES and Third party Auditor.

ABSTRACT

Cloud computing came into importance because of its salient features supporting large amount of users to store and share their files and services. Data security is one of the concerns to be considered while dealing with cloud. Various encryption techniques can be used to enhance data security. The Advanced Encryption Standard (AES) is one of the most recent and efficient encryption schemes which are used by the Cloud and the Third-Party Auditor in order to provide data security and auditability. By the process of public verifiability by a Third-Party auditor, the users can ensure the correctness of data that is being stored in the cloud. In this paper, correctness of data that is being stored in the cloud has been enhanced by the involvement of third-party auditor and AES encryption technique.

***Citation*:** Nikhitha K. Nair and Navin, K. S. 2015. "Enabling and enhancing public verifiability of cloud data using third party auditing", *International Journal of Current Research,* 7, (5), 16008-16010.

INTRODUCTION

The introduction of cloud in recent years which is provided by different service providers, is the service or facility of different components or resources such as hardware, software, storage, platform and it is gaining importance in the field in the field of information technology since it provides freedom for the users from the maintenance perspective on the investment of money for utilizing these services provided by different cloud service providers. Since large amount of users gets involved in sharing and accessing these services and resources which are provided by different cloud service providers, the infrastructure should be capable enough to support them. The service availability, availability of data through any devices which includes the use of browser facility and data synchronization among different devices makes the cloud to be an attractive domain. Now the information is shared and stored in the cloud service providers' area, the clients have the fear about the data privacy, even though certain agreements are made between the clients and the cloud service providers. The term cloud is of importance not to single clients but to different organizations as well.

Corresponding author: Nikhitha, K. Nair,
Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram-695543.

In the case of organization, the concern about the data security becomes multifolded. If we consider an organization containing the departments such as marketing, finance and HR, the data of finance department is considered to be highly sensitive and should be kept highly confidential. Therefore security if these finance details involves high security because it gets uploaded in the cloud. Suppose such data in the cloud gets leaked and tampered, there should be some mechanism for verifying such data. Auditing by a third-party auditor provides some kind of verification. So clients must be able to store the data securely, verify such data and share the data among different users.

Related Work

In this section, review being made related to works addressing auditing and security in cloud. Data security and verification is of great importance while dealing with cloud data. In paper (Deyan and Hong, 2012), the data security is the major challenge in the field of cloud computing since large amount of user's data get stored in the cloud servers which are remotely situated elsewhere and far away from the end users. These data include confidential data and personal data which may be disclosed to public.

In paper (Wang *et al.,* 2009), there is a third party auditor for verification of cloud data. They describes three network entities namely the client which are the users, the cloud storage server which is provided by the cloud service providers and the third party auditor which acts like the verifier for the cloud data. The third party auditor has the public key act with only trusted server and they are not focusing on data privacy. In paper (Wang *et al.,* 2012), it provides two basic schemes. In scheme 1, the user computes the MAC of every file that is to be stored in the cloud. Then client then transfers the files and codes to the cloud and shares the key with the TPA for auditing purpose. During the Audit phase, TPA requests files from the cloud servers and their corresponding MAC to verify the data stored in the cloud. The problem with this scheme is that the TPA can see the entire cloud data. In scheme 2: during the Set Up the user uses s keys and computes MAC for the file blocks and shares the MAC and keys with the TPA. During the Audit phase, TPA gives one of the s keys to the cloud service provider and requests for the MAC from the cloud. So the TPA does not see the entire data that are stored in the cloud. But the problem with this scheme is that a key can be used only once and generating and remembering these large numbers of keys reduces its efficiency.

Proposed Work

In this paper, TPA will be able to maintain confidentiality and audit the integrity of data being stored in the cloud and integrate with the random mask technique to ensure privacy of cloud data while keeping entire data requirements in mind. Encryption technique using AES is also being performed on stored data in cloud to enhance security. The proposed system consists of the following modules.

A. Login Module

In this module, there can be multiple logins namely client login, cloud service provider login and TPA login. The role of client is to store the data in the cloud which are to be shared with other users. The cloud then performs encryption on the data stored using AES encryption technique. The role of TPA is to perform encryption using AES encryption on the encrypted data and perform integrity validation on the data being stored in the cloud.

B. Auditing Module

In this module, TPA performs auditing on the data being stored in the cloud using challenge and response protocol. TPA performs encryption using AES encryption standard on the encrypted data and then store it in the cloud. TPA also performs auditing to ensure integrity on the data being stored in the cloud.

C. Encryption Module

In this module, encrypting the data that is stored in the cloud is being performed by the cloud and also by the TPA. When client store the data in the cloud, the cloud first encrypts the data using AES encryption standard .Then TPA encrypts that data using AES encryption standard. Hence dual security can be provided to the cloud data.

MATERIALS AND METHODS

In this paper, data storage and sharing services in the cloud includes three main entities namely the users, the cloud and the third party auditor.

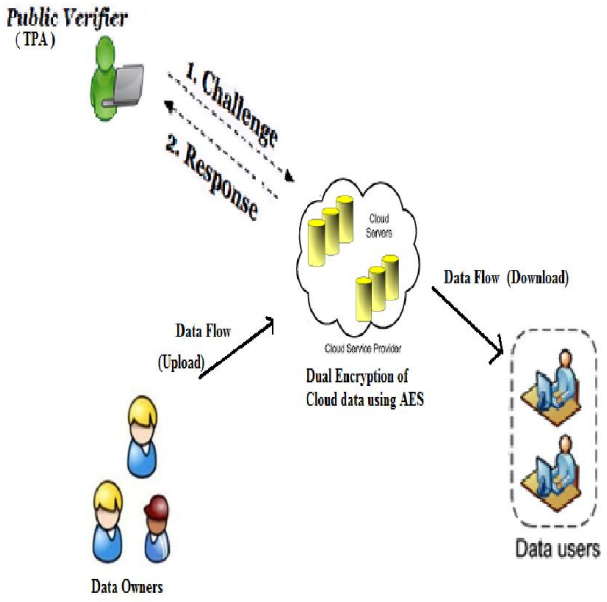

Figure 1. System Architecture

The users include a group of users who actively participate in the data storing and sharing. The original user is the owner of data that are to be stored in the cloud. Considering an organization involving senior scientists and junior scientists where senior scientists are the owners who are capable of uploading their files in the cloud while junior scientists are the users who are capable of downloading the entire data from the data. When the owner stores their data in the cloud, the cloud performs encryption on that data using AES encryption scheme and stores that encrypted data back to the cloud. The TPA then performs dual encryption on that data using AES encryption scheme based on challenge and response protocol. When the user wants to check the integrity of data being stored in the cloud, the users send an auditing request to the TPA. After receiving the auditing request, TPA sends an audit message to cloud and receives an auditing proof of data in the cloud. The TPA verifies the auditing proof. Finally, after the auditing process, TPA provides an audit report to the users indicating the proof of correctness and their integrity.

Conclusion

Cloud computing is the domain that is filled with large number of challenges and this area is of paramount importance. This is the area where large number of users can store their files or share services with other large collection of users. This area provides the users with flexibility to store their files in cloud servers rather than their local machine which utilizes more memory and space. The various encryption techniques can be provided for secure communication between the cloud service providers and users. Auditing is also an important mechanism which is required by the users who are utilizing the cloud services. Third party auditor performs the role of auditing the data that is being stored in the cloud. Advanced Encryption

Standard (AES) is being used for providing dual security on the cloud data by both the cloud and by the TPA. This paper provides enhanced cloud data security with the help of a third party auditor.

REFERENCES

Mayuri V. Badhe and Prabhakar L. Ramteke "Auditor", *International Journal of Computer Science and Mobile Computing*, Vol.4 Issue.1, January- 2015

"Public auditing: Cloud data storage", IEEE Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th *International Conference* –Noida , 26 Sept. 2014, ISBN 978-1-4799-4237-4,

Hemant T. Dhole, Praful C. Papade and Sachin B. Bhosale "Ensuring Data Storage Security using Cloud Computing", *International Journal of Advance Research in Computer Science and Management Studies*, Volume 2, Issue 1, January 2014, ISSN: 2321-7782.

Lifei Wei , Haojin Zhu , Zhenfu Cao Xiaolei Dong , Weiwei Jia , Yunlu Chen and Athanasios V. Vasilakos "Security and privacy for storage and computation in cloud computing", *Elsevier Information Sciences*, Volume 258, 10 February 2014.

Manasi Doshi and Swapnaja Hiray, "Developing Third Party Auditing Scheme for Secure Cloud Storage Service", *International Journal of Computer Applications* (0975 – 8887) Volume 81 – No 18, November 2013

Balakrishnan S and Saranya G "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", *International Journal of Computer Science and Technology*, Volume 2(2), 397–400.

Deyan, C. and Z. Hong, "Data Security and Privacy Protection Issues in Cloud Computing", *International Conference on Computer Science and Electronics Engineering* (ICCSEE), 2012 pp. 647- 651.

Wang, Q., C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th *European Conf. Research in Computer Security* (ESORICS '09), pp. 355-370, 2009.

Wang, C., S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012.

****