International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 3 Issue 3, March 2015

Utilizing AES and XOR Encryption Scheme for Enhancing Data Security and Promoting Data Auditability in Cloud

Nikhitha K. Nair[1], Navin K. S.[2], Soya Chandra C. S.[3]

[1]Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram-695543, India
[2]Department of Computer Science and Engineering, L.B.S. College of Engineering, Poojapura Thiruvananthapuram- 695012, India
[3]Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram-69554, India

Abstract: ***Cloud computing provides the facility for the users to store huge amount of information in the cloud without any requirement to store a local copy of their data in their remote machine. The data, services and resources stored in the cloud can be shared among large amount of users through the internet. This makes data accessibility, data sharing and communication process more flexible and efficient. But main concern dealing with the cloud services include data security, data privacy and authentication issues. Different encryption techniques can be used to handle such problems to a great extent. Auditing enhances the possibility to ensure correctness in the cloud data.***

Keywords: Cloud, Encryption, AES, XOR, Auditing.

1. Introduction

The cloud computing is considered to be a next generation scenario for computing purpose. The cloud computing provides the ease with which different users can easily store their data in the cloud and which promotes data sharing to a larger extent. In recent years, the cloud computing put forward the challenge of storing large amount data in cloud , rather than in their local machine. When the clients store the data in their personal location, the organizations had greater control over that data. But now when the data are stored in remote locations, organization control over that data greatly reduces. Hence there comes the concern about the security and privacy of data being stored in the cloud.

2. Problem Definition

When considering a large organization such as Indian Space Research Organization (ISRO), large number of data owners and data users are involved. These may include senior scientists, junior scientists and engineers of different departments such as mechanical, computer science, finance and electrical. When these users have to store data related to their work details among each other and store such details in their local machine becomes a tedious task. Instead such data can be stored in the cloud server and efficient sharing of services can be made each time. The problems arise regarding the security, privacy and confidentiality of data being stored in the cloud server since they are being stored in remote machine rather than in their local machines.

3. Objective of Proposed Work

The main objective of proposed work is to provide tight security to the data being stored in the cloud. So encryption techniques such AES and XOR encryption schemes are being conducted both by the data owner side and data user side. This paper also attempts to bring in front the scenario of public auditability by a third party auditor in order to verify the integrity of cloud data

4. Methodology

The entire system works in order to provide high security to cloud data. Here security is being provided in terms of encryption techniques. The system works as follows: The owner who wants to store the data in the cloud, encrypt such data using AES encryption standard. Then after encryption, indexing is being done that data. The encrypted data and the index are being stored in the cloud. The users can download the data stored in the cloud based upon their request. In order to provide keyword privacy, XOR encryption scheme is being done by the data users. Also, auditing is being emphasized here to verify that the data stored in the cloud is correct. Here auditing function is being performed by the third party verifier. The third party verifier performs auditing depending upon the users request and generates an audit report indicating the proof giving the correctness of data in the cloud to the users.

5. Scenarios in Design

A. Data Upload Scenario

This Scenario provides the idea about the entire process that takes place during the uploading of data in the cloud by the data owner. The data owner has to register in order to upload his/her data to the data. He then encrypts his data using AES encryption standard. The data owner can re-upload his files whenever needed. He can also view the uploaded and downloaded files from the cloud.

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 3 Issue 3, March 2015

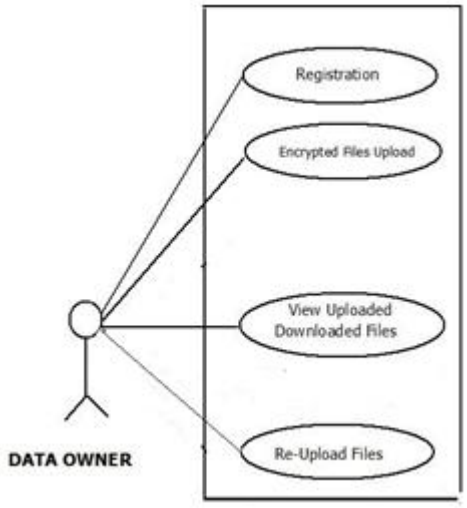

Figure 1: Data Upload Scenario

B. Data Download Scenario

This Scenario provides the ides about the entire process taken place during the downloading process by the clients. The data user in order to download files from the cloud, he has to register himself. The data user performs XOR encryption in order to perform keyword search. The data user can download his files from the cloud based on the ranked responses from the cloud.

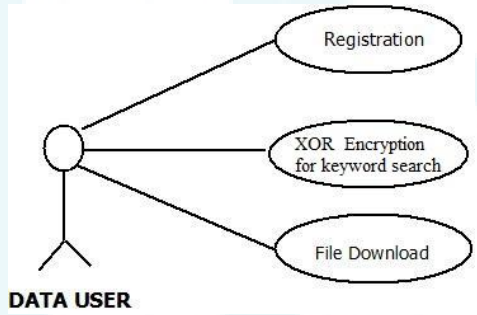

Figure 2: Data Download Scenario

C. Third Party Scenario for Auditing

This scenario provides entire details about the data that is being performed by the third party auditor in order to perform the task of auditing. The third party auditor must first undergo the process of registration in order to prove its identity. Then he performs the task of auditing. Finally, the third party auditor generates an audit report for the clients indicating his proof of correctness of data/files being stored in the cloud.

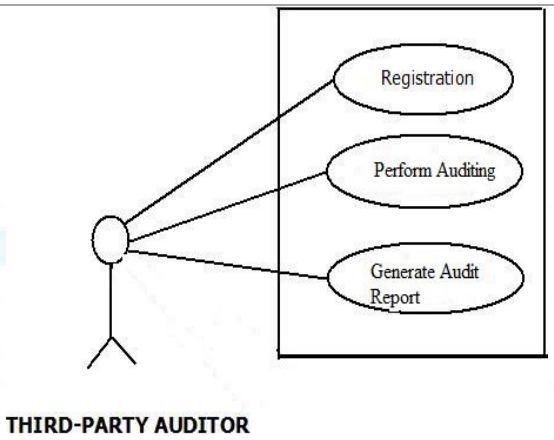

Figure 3: Auditing scenario

6. Conclusion

Cloud computing is one of the emerging technology where most of the work is being carried out every day. Cloud computing provides us with sufficient requirements which help us to store and share data efficient. But together with these facilities, security of data that is stored in the cloud is also an important parameter to be concern .Encryption techniques is the widely used mechanism to deal with security related factors for the cloud data. Also auditing mechanisms are being conducted to ensure integrity of data being stored in the cloud.

7. Future Enhancement

The security on cloud data can be enhanced by using more advanced encryption standards such as homomorphic scheme. The combination of various encryption techniques that are being used together also provides strict security. Encryption techniques can also be provided at different level of entire process.

References

[1] Cong Wang ,Chow, S.S.M., Qian Wang ,Kui Ren ," Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on computers, Vol. 62, No. 2, February,2013.
[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, Apr, 2011.
[3] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.
[4] Cong Wang, Ning Cao, Kui Ren and Wenjing Lou," Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE Transactions on Parallel and Distributes Systems, Vol.23, NO.8, AUGUST 2012).
[5] Ankatha Samuyelu Raja, Vasanthi A, "Secured Multi-keyword Ranked Search over Encrypted Cloud Data", International Journal of Advanced Research in Computer Science and Software Engineering-Volume 2, Issue 10, October 2012)