International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Dual Security Using Dual Encryption Schemes and Efficient User Revocation in Cloud

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

[1]Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram-695543

Abstract: ***Cloud computing in the domain of distributed systems introduces many challenges in the day-to-day life. One of the main challenges is data security and privacy. Security on cloud data can be enhanced using dual encryption. Different encryption techniques such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES, Exclusive-OR (XOR), Rivest, Shamir and Adleman (RSA) are used for this purpose. The encryption techniques such as Exclusive-OR (XOR) and Advanced Encryption Standard (AES) can be used together to perform dual encryption on the cloud data. By utilizing cloud to re-sign the blocks that were previously signed by the revoked user on behalf of existing users, efficient user revocation can be performed. Auditing by the Third party auditor ensures the integrity of data stored in the cloud.***

Keywords: Cloud computing, Dual encryption, User- Revocation, Third-party Auditing**.**

1. Introduction

The introduction of cloud computing in the domain of distributed systems brings in front, a model that enables convenience and on-demand network access to a pool of computing resources which can be shared such as networks, storage, servers and services) and which can be easily provisioned and released with minimum service provider interaction .

Cloud used can be a public cloud, private cloud or even a hybrid cloud. In public cloud, services are offered over the internet and a cloud provider owns and operates it. In the case of private cloud, the whole cloud infrastructure is operated and managed only for a specific organization. A hybrid cloud is combination of different cloud for resource sharing.

Cloud computing brings in front, numerous challenges as more data owners and data users are involves, and data is stored in offsite locations. When it comes to cloud computing, the security and privacy of personal information is extremely an importance. The need for encryption of data to be stored in cloud, issues relating to data ownership, guarantee towards quality of service are some of the challenges commonly faced while dealing with cloud data.

This paper introduces the idea of dual encryption using Exclusive-OR (XOR) encryption standard and Advanced Encryption Standard (AES) on cloud data which are stored in cloud by data owners for sharing. With single encryption, expert users can easily decrypt the data and reduce its essence. So, there is a need for dual-encryption to be provided on the data.

The data owners who use the cloud for storage first perform encryption using Exclusive-OR (XOR) Encryption Scheme. The cloud after receiving the encrypted data then performs dual encryption using Advanced Encryption standard (AES). Dual encryption enhances security on cloud data.

The Identity Protocol issue tokens to users based on their identity attributes for user account verification. For data owners to upload their encrypted data in the cloud, Identity protocol should grant permission by verifying the user account details.

Efficient revocation of users from the cloud is another problem that is to be considered while dealing with cloud computing. When the data owner uploads the encrypted data in the cloud, data is stored in the cloud as blocks which are signed by them. So, when a user is revoked from the cloud, blocks which are signed by the revoked user, must be re-signed by the existing users. Here cloud re-signs the blocks of revoked user on behalf of existing users [4].

Auditing of data stored in the cloud by a third party is a necessity while handing cloud data. Third-Party Auditor (TPA) will perform the process of auditing of cloud data on request from the data users to ensure integrity of data stored in the cloud.

This paper aims to bring forth the following objectives:

a) Dual encryption on data to provide additional security using Exclusive-OR (XOR) Encryption scheme and Advanced Encryption Standard (AES) Re-signing the shared blocks by the cloud on behalf of existing users, so the existing users do not need to download and re-sign the blocks by themselves during user revocation.
b) Auditing of shared data by third-party auditor (TPA) to check the integrity of shared data.

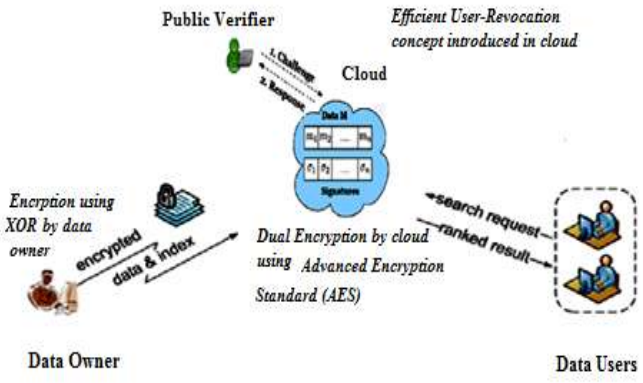

Figure 1: System Architecture

The remaining portion covered in this paper includes: In Section II, system model and design goals are introduced. Section III describes the proposed system. Section IV covers the methodology of entire system working, followed by Section V, which describes the framework. Finally, the paper is concluded in Section VI.

2. Problem Formulation

A. System Model

Considering the Figure 1: There are four entities namely-the data owner, the data user, the cloud server and the third-party auditor (TPA). The data owner sends the encrypted data along with an index to the cloud server. The cloud server performs dual encryption and stores that encrypted data in the cloud. The encrypted data are stored in the cloud as blocks which are signed by the respective data owners.

Upon receiving the search request from the data users, the cloud server is responsible to search the index and return the corresponding set of encrypted data. The data user has to perform dual-decryption in order to obtain the original data. The third-party auditor (TPA) performs auditing on the cloud data upon the request from the users through challenge-response protocol.

B. Design Goals

Our system design should guarantee security and integrity of data as follows:

1. Multi-keyword Ranked Search:
To design search schemes, which allow multi-keyword search request with effective search results, rather than unordered results.

2. Dual Encryption using Exclusive-OR (XOR) Encryption Scheme and Advanced Encryption Standard (AES) for data privacy:
To prevent data that is stored in the cloud being hacked, security is being provided to such data through these modes of encryption.

3. User Revocation:
System employs efficient user-revocation concept using proxy re-signature scheme to overcome the situation when a user is revoked from the cloud.

4. Auditing:
Third party auditor (TPA) audits the integrity of shared data that is being stored in the cloud, without retrieving the entire data from the cloud.

3. Proposed System

"Dual encryption" performed on the data sent by the data owner to the cloud for storage is introduced in this paper. In "Single encryption", expert users can easily decrypt the data and reduce its essence. So, there is a need for dual encryption to be provided for the data. When the data owner sent encrypted data along with the index-key to the cloud for the data users, then dual- encryption is performed on the data by the cloud, so that even the expert cannot decrypt the data easily. Here key generation is through "Attribute Based Key Generation Technique".

The data that is sent by the data owner to the cloud is first encrypted using **XOR** (**Exclusive-OR).** The Cloud then performs **AES** (Advanced Encryption Standard) on the encrypted data sent by the data owner that indicates dual security of data stored in the cloud. The data user then should perform dual decryption in order to retrieve the original data stored in the cloud.

System employs "**Multi-keyword Ranked search**", in which multiple keywords can be given as search string by the data user. It considers the frequency of occurrence of the search word. Based on the number of occurrences, relevant response is returned to the data users.

System employs "**Efficient User- Revocation concept**" which introduces the condition when a user is revoked from the cloud. By using the idea of proxy re-signatures, cloud re-signs the blocks on behalf of existing users in the cloud.

System uses "**Identity Protocol** (IdPs)" that issue identity tokens to users based on their identity attributes for user account verification. For data owners to upload their encrypted data in the cloud, IdPs should grant permission to them.

In addition, a **public verifier (Third-Party Auditor)** is always able to audit the integrity of shared data without retrieving the entire data from the cloud. The auditing process is through challenge-response protocol.

4. Methodology

The entire system works as follows:

When the data owner wants to outsource the data collection to the cloud server, the data owner performs encryption on the data using XOR (Exclusive-OR) Encryption standard and

generates a private key (owner key) using Attribute-based key generation technique.

To enable searching and efficient data retrieval, the data owner before outsourcing, will first build an index for searching from the data collection and then outsource both the index and the encrypted document collection to the cloud server.

The Identity protocol then performs data owner verification before allowing the data owner to outsource the data to the cloud. The identity protocol then grant identity tokens to the verified data owners which become their identity. Then the files of verified data owners are forwarded by the Identity protocol to the cloud for storage.

The cloud when receives the encrypted data of the data owner forwarded by the Identity protocol, the cloud performs dual-encryption using Advanced Encryption Standard (AES) on them and generates a cloud key.

Upon receiving the search query from the data users, the cloud server is responsible to search the index and return the corresponding set of encrypted documents. Based on the frequency of occurrences of search keyword, relevant response is returned.

The data users when receives the required files according to their search query, they must first decrypt the encrypted files (First decryption) using the cloud key and then again decrypt the files (Second decryption) using the owner key. Then only they can retrieve the original data sent by the data owner. There by dual security is provided.

During owner key generation by the data owner, who is the creator of shared data, also creates a user list, which contains ids of all the users in the group. The user list is public and signed by the data owner.

When the data owner creates shared data in the cloud, he/she computes a signature on each block. After that, if a data owner in the group modifies a block in the shared data, the signature in the modified block is also computed.

When a user is revoked from the group, the cloud re-signs the blocks, which were previously signed by this revoked user with a re-signing key

Having the public key, signature of the block, block identifier and the block itself, the cloud (proxy) performs verification and then converts this signature with its own piece of the corresponding re-signing key. Finally, after the re-signing process in the cloud, the original user removes user's id from the user list and signs the new user list.

In addition, when a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message or challenge to the cloud, and retrieves an auditing proof (response message) of shared data from the cloud. Then the TPA verifies the correctness of the auditing proof after having the auditing message, an auditing proof and all the existing user's public keys [6]. Finally, the TPA sends an auditing report to the user based on the result of the verification.

5. Framework

The entire system works according the following algorithm:

1. **Generate Key:** Private keys are being created by every user in the group.
2. **Create Signature:** Having the private key and block identifier, signatures are being created by the data owners before uploading shared data in the cloud.
3. **Encryption using XOR:** Data is being first encrypted using Exclusive-OR (XOR) Encryption scheme by the data owners before uploading their data in the cloud.
4. **Generate Cloud Key:** The cloud computes a cloud key by performing dual encryption on the encrypted data using Advanced Encryption Standard (AES).
5. **Generate Re-Signatures:** Having the cloud key, signature, block and block identifier, the cloud computes re-signatures on behalf of existing users when a user is revoked from the cloud.
6. **Proof Generation:** A public verifier generates an auditing message and sends it to the cloud. After receiving the auditing message, cloud generates a proof of possession of shared data.
7. **Proof Verification**: Having the auditing message, auditing proof and all the users cloud keys, the public verifier verifies the correctness of auditing proof.

6. Conclusion

In this paper, proposed a dual encryption technique on cloud data to enhance security. The data send by the data owner is first encrypted using "XOR (Exclusive-OR) Encryption scheme". The key generation is through Attribute based key generation technique. The encrypted data along with the index and signature is uploaded to the cloud for storage. But before uploading, the Identity protocol (IdP) should grant permission by verifying user identity and grant user with identity tokens. The data owner uploads the encrypted files to the cloud after generating signatures to recognize their blocks of files. The cloud then performs dual encryption on cloud data using "Advanced Encryption Standard (AES)". The data users can download files by searching their request. The Cloud re-signs the blocks which were signed by a revoked user, on behalf of existing user during user revocation. Third-Party Auditor also plays a major role in the verification process during auditing.

References

[1] 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, 2013.
[2] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud

Definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50-55, 2009.

[3] S. Kamara and K. Lauter,"Cryptographic cloud storage," in *RLCPS, January 2010, LNCS.Springer, Heidelberg*.

[4] 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.

[5] 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).

[6] Boyang Wang, Baochun Li and Hui Li,"Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Transactions on service computing NO:99 VOL:PP YEAR 2014.

[7] Zhiyong Xu, Wansheng Kang, Ruixuan Li, KinChoong Yow, and Cheng-Zhong Xu," Efficient Multi-Keyword Ranked Query on Encrypted Data in the Cloud", IEEE 18th International Conference on Parallel and Distributed Systems.

[8] S. Usha, Dr.A.Tamilarasi and R. Vijayakumar," Support Ranked Keyword on Remote Encrypted Data in Cloud", (International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013).

[9] Ankatha Samuyelu Raja and 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.

[10] M. Suriyapriya1, A. Joicy, "Attribute Based Encryption with Privacy Preserving In Clouds" , International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 2 231 – 236.

[11] Manasi Doshi , 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.

[12] Miss. Nupoor M. Yawale1, Prof. V. B. Gadicha," Third Party Auditing For Secure Data Storage in Cloud through Trusted Third Party Auditor Using RC5", International Journal of Application or Innovation in Engineering & Management (IJAIEM) ISSN 2319 – 4847, Volume 3, Issue 3, March 2014.