International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Implementation of Robust Multi owner Multi group Data Security Algorithm for Cloud Environment

Charanraj B R[1], K.R. Shylaja[2], Ravinandan M E[3]

[1]M.Tech IV Sem, Department of CSE, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India

[2]Associate Professor, Department of CSE, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India

[3]Teminnova Technologies Private Limited, Bangalore, Karnataka, India

Abstract: ***Cloud computing is a kind of centralized database where number of clients accumulate their data, recover data and possibly adjust data. Concerns of sensitive information on cloud potentially cause privacy problems. Data encryption protects data security to some extent so have to use Blowfish-AES encryption and zip an encrypted files before uploading for reduce memory space. Multi owner scheme (MOS) for data sharing by supporting dynamic groups efficiently so that revocation can be easily achieved. This guarantees any member in a group to anonymously utilize the cloud resource, so security issues rapidly arises when group owner adopted this Multi owner scheme.***

Keywords: Cloud, Blowfish-AES encryption, group signature, revocation, Zip method.

1. Introduction

Cloud computing has now emerged to become one of the best methods for companies wanting to revamp and enhance their IT infrastructures. However, there are certain issues and problems associated with cloud computing. Needless to say, it is very advantageous for everyone to adapt to new technology, but it is also wise to recognize some of the risks associated with this technology. The cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters [4].

A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [3].

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner [1],[5]. Compared with the single-owner manner [2], [6]. Groups are normally dynamic in practice. an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

In this paper, using the Blowfish and AES algorithm for encryption and used group signature for authentication purpose. And for save memory space has to use zip a file before uploading an encrypted files to the cloud server.

2. Preliminaries

2.1 Overview

Four different entities are involved in Figure. 1, such as the cloud server, Admin, group manager (i.e., the company manager), and a large number of group members (i.e., the staffs).

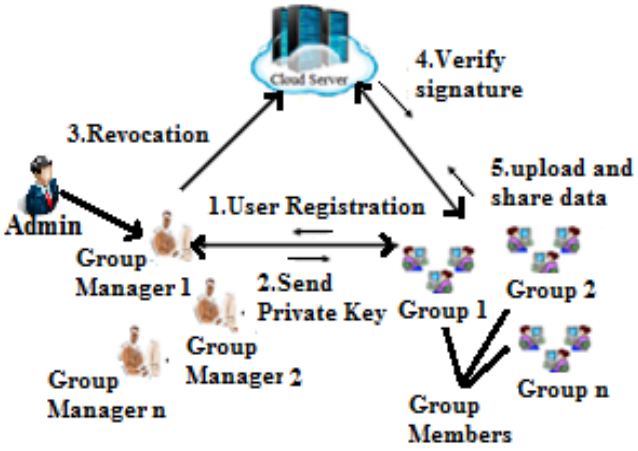

Figure 1: System model

Cloud server is operated by cloud service providers and the fundamental service provides by them as storage as a service. However, the cloud is not fully trusted by users. The cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes.

Admin is responsible for groups and group managers because admin only create that groups and group managers.

Group manager is responsible for system parameters generation, registering the new member, revocation the member and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by

the administrator of the company. Therefore, assume that the group manager is fully trusted by the other parties.

Group members are the registered members they will Store their private data into the cloud server and share the data among the group members. For example, the staffs play the role of group members. It allows the group members to be dynamically changed, due to the staff resignation and the participation of new staffs in the company.

2.2 Group Signature

A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability. In this paper, a variant of the short group signature scheme will be used to achieve anonymous access control, as it supports efficient membership revocation.

3. Problem Statement

DES (Data Encryption Standard) is a symmetric algorithm. It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation; 8 bits are used for error detection DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text. DES was not designed for software and hence runs relatively slowly. The 56-bit key size is the biggest defect of DES because 56-bit size being too small. A group of computer experts collaborated to publicly break a DES key in 22 hours & 15 minutes. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. DES is easily crackable.

4. Algorithm Principles

4.1 Blowfish and AES

Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less. Blowfish encryption is that it is one of the strongest the speed of the algorithms and key strength is also algorithms available and the speed of the algorithms and key strength is also very good.

Blowfish is a fast block cipher, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text. In one application Blowfish's slow key changing is actually a benefit: the password-hashing method used in OpenBSD uses an algorithm derived from Blowfish that makes use of the slow key schedule; the idea is that the extra computational effort required gives protection against dictionary attacks.

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and combination, and is fast in both software and hardware. The data path is shown in Figure. 2.

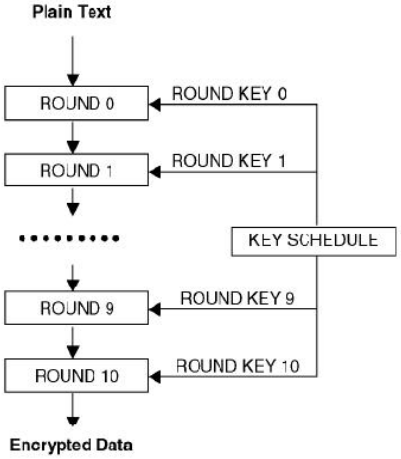

Figure 2: the data-path for data block & key size of 128bits.

a) **Key Expansion-**round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more. Generic structure of one internal round is shown in Figure. 3.

b) Initial Round-AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

c) Rounds

- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

d) Final Round (no MixColumns**)**

- SubBytes
- ShiftRows
- AddRoundKey.

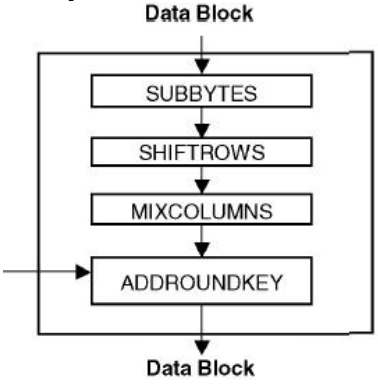

Figure 3: Generic structure of one internal round

4.2 Signature Generation Algorithm

Input: Private key (A, x), system parameter (P, U, V, H, W) and data M.
Output: Generate a valid group signature on M.
begin

Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
Computes the following values

$$\begin{cases} T_1 = \alpha \cdot U \\ T_2 = \beta \cdot V \\ T_3 = A_i + (\alpha + \beta) \cdot H \\ R_1 = r_\alpha \cdot U \\ R_2 = r_\beta \cdot V \\ R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U \\ R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V \end{cases}$$

Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
Construct the following numbers

$$\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_x = r_x + cx \\ s_{\delta_1} = r_{\delta_1} + c\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2 \end{cases}$$

Return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
end

A **signature generation** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity) [2].

Signature Verification Algorithm

Output: True or False.
begin

Compute the following values

$$\begin{cases} \tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R}_2 = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R}_3 = (\frac{e(T_3, W)}{e(P, P)})^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta} \\ \qquad e(H, P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases}$$

if $c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$
Return True
else
Return False
end

The hash functions are used for signature generation and verification methods and how it will be works is shown in Figure. 4.

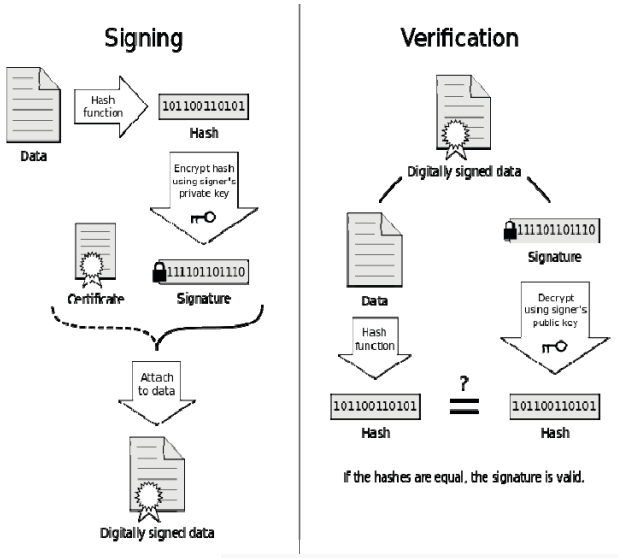

Figure 4: Process of signature is applied and then verified

4.3 Revocation Verification Algorithm

Input: System parameter (H_0, H_1, H_2), a group signature σ, and a set of revocation keys $A_1, ..., A_r$
Output: Valid or Invalid.
begin

set $temp = e(T_1, H_1)e(T_2, H_2)$
for $i = 1$ to n
if $e(T_3 - A_i, H_0) = temp$
Return Valid
end if
end for
Return Invalid
end

5. Design

5.1 Admin

1) Admin login with valid credentials.
2) Then create group and group and group manager.
3) For Each Group one directory must be created by Group Name in cloud storage.
4) Each Group must have unique Group Private Key for Encryption & Decryption (AES).

5.2 Group Manager

1)Group manager login with valid credentials.
2)Then create group members and private key for each group members.
3)Given private key have GID (Group ID), MID (Member ID), GPK (Group private key).
4) Encrypt the private key using Blowfish algorithm and send that encrypted private key to each group members.
5)Group manager have authority to group member revocation,

- List the Member.
- Select the Member to be revoke.
- Add the member ID in Revocation List.

5.3 Group Member

1) Group Member login with valid credentials.
2) First, group member decrypt the private key using Blowfish algorithm.
3) Then get the decrypted private keys which have GID, MID, GPK.
4) The given GPK (Group Private Key) is generated by using AES algorithm. By using this GPK, have to encrypt a files before uploading to the cloud server.
5) Create a signature and update it in database.
6) Then compress an encrypted file to ZIP method and upload into the cloud server.
7) When group members want to download a file that will be restricted for that group members only. So first, decrypt the private key and get the GID, MID, GPK.
8) Then check the GID, if it fails then that will be rejected and listed in revocation list based on GID.
9) If GID is succeed then verify UID and get the signature for each downloading file.
10) Decompress the ZIP file then get an encrypted files.
11) Then have to enter private key for decrypting an encrypted files using AES algorithm.

6. Performance Analysis

In this paper, the future scope of the study should be the storage overhead and encryption computation costs of scheme are independent with the number of revoked users. The user list and the shared data list should be stored at the group manager. By using that Zip method has to reduce the memory space in storage. Each user only needs to store its private key. By using this Blowfish and AES encryption the security should be in the key, and both of these algorithms are resistant to brute force attacks. Blowfish uses all 448 bits of the key, so a brute-force attack would take on average 2447guesses at the key, whereas AES would take 2255 guesses on average.

6.1 Security Requirements

Data confidentiality is the assurance that data cannot be viewed by unauthorized users including the cloud is incapable of learning the content of the stored data. And data confidentiality is to maintain its availability for effective groups.

Access control is the assurance that Group members are able to use the cloud resource for data operations. Unauthorized users cannot access the cloud resource at any time, and revoked users will be unable to use cloud once they are revoked.

Traceability is the assurance that group members can access the cloud without revealing the real identity. And traceability represents an effective protection for user identity

Efficiency is the assurance that any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

7. Conclusion

In this paper, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, it supports efficient user revocation and new user joining. Efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. For secure purpose have to use Blowfish and AES encryption and for reduce the memory space have to apply zip method on an encrypted files.

References

[1] M Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[2] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.
[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz,A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
[6] Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

Author Profile

Charanraj B R received the B.E. degree in Information Science Engineer from RNSIT, Bangalore and pursuing MTech degree in Computer Science and Engineering from Dr. Ambedkar Institute of Technology, Bangalore in 2012-2014. He has strong passion for Computer Networks and Cloud Computing.

K.R. Shylaja received MTech degree in Computer Science from Visvesvaraya Technological University. She is currently perusing her Ph.D from JNTU, Kakinada, Andhra Pradesh, India. She has 14 years of experience as lecturer and Asst. Professor, Currently she is an Associate Professor, Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology, Bangalore.

Ravinandan M E received B.E degree in Computer Science Engineer from Bangalore University, MTech degree in Computer Science & Engineering from VTU. He had served as a scientist in DRDO and GE Healthcare. Currently he is MD & CEO of Teminnova Technologies Private Limited and also a Founder Member of Organization for Rare Diseases India.