ISSN 2348 – 7968

Secured Data Sharing For Dynamic Groups In Cloud Computing

Siddhant Hinge, Yuvraj Pachpind, Rakesh Yendhe

Department of computer engineering, Savitribai Phule University of Pune, Maharashtra, India

Abstract

cloud computing provides an economical and efficient solution for sharing data among cloud users. sharing data in a group while preserving data and privacy from an cloud is still a big issue. Hence to maintain the data security is very important on cloud for protecting the data. Because of this issue data encryption is necessary. We can also communicate using encrypted message service among cloud users.

Keywords : *Cloud computing, data sharing, privacy-preserving, access control, encrypted message*

1. Introduction

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. 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**.**

To achieve secure data sharing for dynamic groups in the cloud, we combine the group signature and dynamic broadcast encryption techniques. Specifically, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users which protects the confidentiality from the revoked users in the dynamic broadcast encryption scheme.

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage.
The character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a group manner while preserving data and privacy from an un-trusted cloud is still a challenging issue, due to changes in cloud users.
We can communicate with other users using cloud. In this paper we are proposing to encrypt each and every message sent via cloud using SPEKE algorithm. Using this encryption algorithm we are able to achieve security and privacy.

1.1 Related work

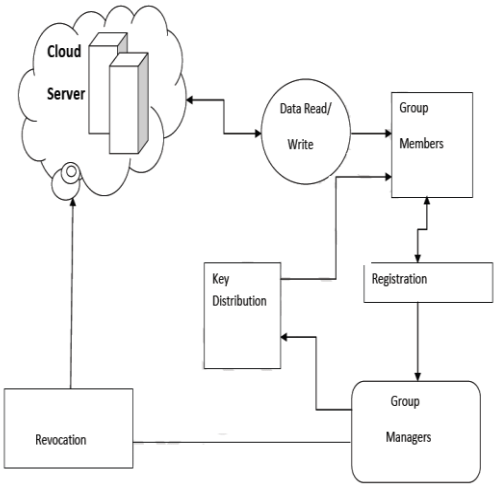
proposed a cryptographic storage
system that enables secure file sharing on untrusted servers, By dividing files into filegroups and encrypting each filegroup with a unique file-block key, the data owner can share the filegroups with

ISSN 2348 – 7968

others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

2. Proposed System logic and Architecture:

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.



Cloud Server:

Cloud is operated by cloud service providers and provides priced abundant storage services.

Group Manager:

Group Manager takes the charge of system parameters like user registration, user revocation, secret key generation.

Group Members:

Group members are the set of registered users that will store their private data into the cloud server and can download it and share the data with others in the group.

3. Mathematical module

Signature generation:

Input: Private key (A,x), system parameter (P,U,V,H,W) and data M.

Begin

Select random number a,b,c,d,e,f,g € z

Compute the following values

T1=a.U

T2=b.V

T3=A1+(a+b).H

R1=c+U

R2=d.V

R3=e(T3,p)e,e(H,W),-c-d,e(H,P)-h-g

R4=e.T1-f.U

R5=e.T2-g.V

Set c=f(M,T1,T2,T3,R1,R2,R3,R4,R5)

Construct the following number

S1=r1+c1

S2=r2+c2

S3=r3+c3

S4=r4+c4

S5=r5+c5

Return Δ=(T1,T2,T3,c,s1,s2,s3,s4,s5)

ISSN 2348 – 7968

End

Signature verification

Output: true or false

Begin

Compute the following values

R1=s1.U-c.T1

R2=s2.V-c.T2

R3=(e(T3,W)/e(P,P))^c*e(T3,P)^S3*e(H,W)^(-s1-s2)* e(H,P)^(-s4-s5)

R4=s3.T1-s4.U

R5=s3.T2-s5.V

If c=f(M,T1,T2,T3,R1,R2,R3,R4,R5)

return True

Else

return False

end

Cloud Computation Cost

To evaluate the performance of the cloud, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB.. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations, since the size of signed message is constant.

Acknowledgments :

The authors thank the editors and guide reviewers for their valuable comments to significantly improve the quality of this paper.

4. Conclusions

We design a secure data sharing scheme, Mona, for dynamic groups in an cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports user revocation and new user joining. More specially, 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. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

5. References

[1] 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.

[2] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[3] 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.

[4] E. 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. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schem

[5] G. es with Applications to Secure Distributed Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

ISSN 2348 – 7968

[6] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.