Preserving a Fine-grained Access Control and Data Integrity on Cloud Storage

U.DEEPIKA[1] **& Y.G.Deepa**[2], **Dr.K.Ramakrishna**[3]

[1]M-Tech Dept. of IT Sridevi Women's Engineering College Hyderabad

[2]Assistant Professor Dept. of IT Sridevi Women's Engineering College Hyderabad

[3] Professor & HOD, Dept. of IT Sridevi Women's Engineering College Hyderabad

Abstract

Cloud storage empowers users to store their data remotely and enjoy the on -demand high quality cloud applications without the burden on local hardware and software management. The data compromise can occur because attack by nodes in the cloud and other users. Therefore, high security area required protecting data in the cloud; we introduce secure and optimal performance approach for data manipulation in cloud. In this methodology, when data owner wants to send file on cloud server first file is dividing into fragments and it then encrypted. These encrypted fragments data over the cloud nodes. Each node stores only one fragment of a particular data file to make ensure even in case that successful attack, no meaningful information is catching to the attacker. We use T-coloring concept for storing the fragments in nodes and separated with certain distance to prevent an attacker is predicting the fragments locations. To maintain integrity we are using the Third Party Auditor (TPA) which makes the audit report stored file on cloud and sent it to the data owner by mail. If attacker modified the file then TPA sends audit report as changed file to data owner and Proxy Agent. Finally proxy Agent which replace the modified code with original contents.

Keywords: cloud security, Cloud Storage, fragmentation, Third Party Auditor (TPA), Performance.

1. Introduction

Cloud storage services have rapidly become popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user confidentiality, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. Most of the planned schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult.

As one example, Lava bit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service. Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored cipher text. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called deniable encryption, first proposed in. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in cipher texts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence.

This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data1. A deniable ABE scheme for cloud storage services. ABE characteristics can be used for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. This scheme is based on Waters cipher text policy attribute based encryption (CP-ABE) scheme.

This scheme enhances the Waters scheme from prime order bilinear groups to Composite order bilinear groups. By the subgroup decision problem assumption, this scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

2. Related Work

2.1 EXISTING SYSTEM:

There are numerous ABE schemes that have been proposed. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets.Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption. There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE).Goyal et al. proposed the first KPABE. They constructed an expressive way to relate any monotonic formula as the policy for user secret keys. Bettencourt et al. proposed the first CP-ABE. This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the cipher text.

DISADVANTAGES OF EXISTING SYSTEM:

It is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satisfy the conditions are able to decrypt the encrypteddata.Use translucent sets or simulatable public key systems to implement deniability. Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case. Most of the previous deniable encryption schemes are inter-encryption independent. That is, the encryption parameters should be totally different for each encryption operation. If two deniable encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility. Most deniable encryption schemes have decryption error problems. These errors come from the designed decryption mechanisms.

2.2 PROPOSED SYSTEM:

In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters cipher text policy-attribute based encryption (CP-ABE) scheme. We enhance the Waters scheme from prime order bilinear groups to Composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers. In this work, we construct a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes.

ADVANTAGES OF PROPOSED SYSTEM:

Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability. Instead, we adopt the idea proposed with some improvements. We construct our deniable encryption scheme through a multidimensional space. All data are encrypted into the multidimensional space. Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. We make use of Composite order bilinear groups to construct the multidimensional space. We also use chameleon hash functions to make both true and fake messages convincing. In this work, we build a consistent environment for our deniable encryption scheme. By consistent environment, we mean that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all cipher texts under this environment, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of our scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, we can construct the released fake key to decrypt normal cipher texts correctly.

3. Implementation

A. Owner Module

Owner module is to upload their files using some access policy. First they get the public key for particular upload file after getting this public key owner request the secret key for particular upload file. Using that secret key owner upload their file.

B. User Module

This module is used to help the client to search the file using the file id and file name .If the file id and name is incorrect means we do not get the file, otherwise server ask the public key and get the encryption file. If you want the decryption file means user have the secret key.

C. Deniable Encryption Module:

Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in cipher texts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing.

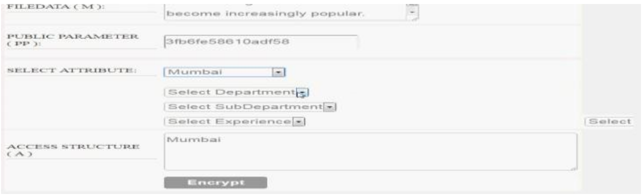
D. Key Distributor Module

We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management. In this module generate public key for related user based on user/owner attribute.

E. Cloud Service Provider

Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption scheme.

4. Experimental Work



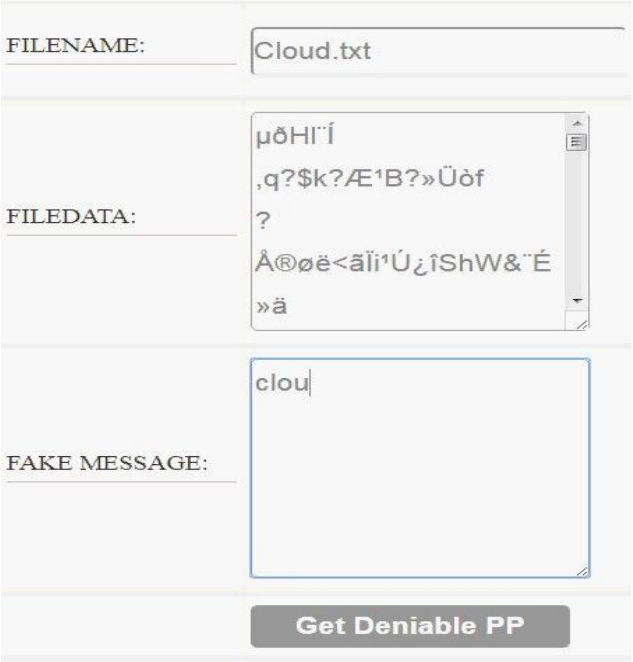
FILEDATA (M): become increasingly popular.

PUBLIC PARAMETER (PP): 3fb6fe58610adf58

SELECT ATTRIBUTE: Mumbai

ACCESS STRUCTURE (A): Mumbai

Fig 1: Access structure and attributes public parameters.

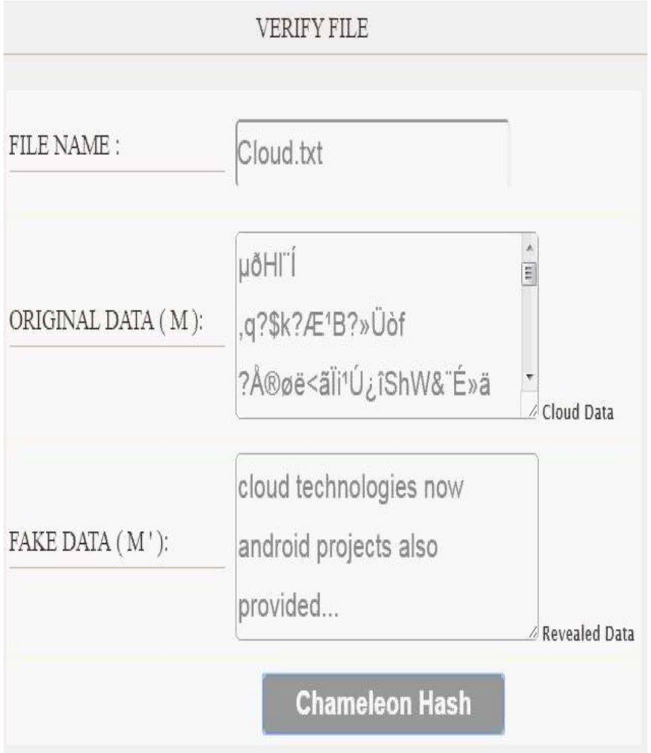


FILENAME: Cloud.txt

FILEDATA: µðHI¨Í ,q?$k?Æ¹B?»Üòf ? Å®øë<ãÏì¹Ú¿îShW&¨É »ä

FAKE MESSAGE: clou

Fig 2: File Data with Encrypted format with fake message.



FILE NAME : Cloud.txt

ORIGINAL DATA (M): µðHI¨Í ,q?$k?Æ¹B?»Üòf ?Å®øë<ãÏì¹Ú¿îShW&¨É»ä

FAKE DATA (M'): cloud technologies now android projects also provided...

Fig 3: Verifying File Data between original Data and Fake Data.

5. Conclusion

A survey work carried out on deniable CP-ABE scheme to construct an audit-free cloud storage service. The deniability quality makes intimidation unacceptable, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Planned scheme provides a potential way to fight beside immoral interference with the precise of confidentiality and more schemes can be created to protect cloud user privacy.

6. References

[1]. A .Sahai and B. Waters, “Fuzzy identity based encryption,” in Eurocrypt, 2005, pp. 457–473.

[2]. GOYAL, O. PANDEY, A. SAHAI, AND B. WATERS, “ATTRIBUTE-BASED ENCRYPTION

FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA,” IN ACM CONFERENCE

ON COMPUTER AND COMMUNICATIONS SECURITY, 2006, PP. 89–98.

[3]. Bowater’s, “Cipher text-policy attribute based encryption: An expressive, efficient, and provably secure realization,” in Public ey Cryptography, 2011, pp. 53–70.R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997.

[4]. S. Rosenberger and B. Waters, “Attributebased encryption with fast decryption,” in Public Key Cryptography, 2013, pp. 162–179

[5]. R. Canetti, C. Work, M. Naor, and R. Ostrovsky, “Deniable encryption,” in Crypto, 1997, pp. 90–104./

[6]. M. D¨urmuth and D. M. Freeman, “Deniable encryption with negligible detection probability: An interactive construction,” in Eurocrypt, 2011, pp. 610– 626. “PDCA12-70 data sheet,” Opto Speed SA, Mezzovico, Switzerland.

[7]. B. Lewko, “Tools for simulating features of composite order bilinear groups in the prime order setting,” in Eurocrypt, 2012, pp. 318–335.

[8]. D. Boneh, R. Canetti, S. Halevi, and J. Katz, “Chosen-ciphertext security from identitybased encryption,” SIAM J. Comput., vol. 36, no. 5, pp. 1301–1328, 2007.

[9]. K. Liang, L. Fang, D. S. Wong, and W. Susilo, “A ciphertextpolicyattribute-based proxy re-encryption with chosenciphertextsecurity,” IACR Cryptology ePrint Archive, vol. 2013, p. 236, 2013