THOMSON REUTERS
ENDNOTE

[Sukanya., 3(4): April, 2016]

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

CLOUD STORAGE FOR PRIVACY PRESERVING USING DENIABLE ENCRYPTION

Sukanya*, Renukaradhya P.C

*PG Student M.Tech Computer Science, ShriDevi Institute of Engineering and Technology Tumakuru, Karnataka, India

Assistant Professor Computer Science, ShriDevi Institute of Engineering and Technology Tumakuru, Karnataka, India

KEYWORDS: Deniable Encryption, Attribute-Based Encryption, Cloud Storage.

ABSTRACT

Cloud storage services have become very popular. Because of the cloud service providers maintains the users data privacy, different types of cloud storage are made available by companies like Google, Apple, Microsoft, etc. helping users with storing important files and documents securely on the internet. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some outside authorities may demand cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether to avoid that unauthorized access a storage encryption scheme enabled. In this paper, I present a design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

INTRODUCTION

Cloud storage is a form of data storage where the digital data is stored in logical pools, the physical storage span multiple servers (and often locations), and the physical environment is typically owned and handled by a hosting organization. These cloud storage providers are answerable for keeping the data available and accessible, and the physical environment protected and running. Different organizations buy or lease storage capacity from the providers to store customer application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a gateway or Web- based content management systems. In the cloud storage environment customers can store their data on the cloud and access their data from anywhere at any time by connecting to a network. Because of user privacy, the data stored on the cloud is normally encrypted and safe guarded 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. Attribute-based encryption is a kind of public-key encryption in which the secret key of a user and the cipher text are reliant upon attributes.

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. Bethencourt 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 ciphertext.

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 encrypted data.

- 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.

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 ciphertext 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 auditfree. 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, ciphertexts 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 means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all ciphertexts 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 ciphertexts correctly.

METHODOLOGIES

- **Deniable Encryption**:

Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts 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.

- **Attribute-Based Encryption**:

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, 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. There are numerous ABE schemes that have been proposed, including 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. 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.

- **Cloud Storage:**

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 schemes. In this project, i present a design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected. 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. 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 ciphertext. 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.

- **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.

- **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 u want the decryption file means user have the secret key.

- **Distributed Key Policy Attribute Based Encryption:**

KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms which is defined as follows

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

Setup:
This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:
It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation:
It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption:
It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message. 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.

IMPLIMENATATION

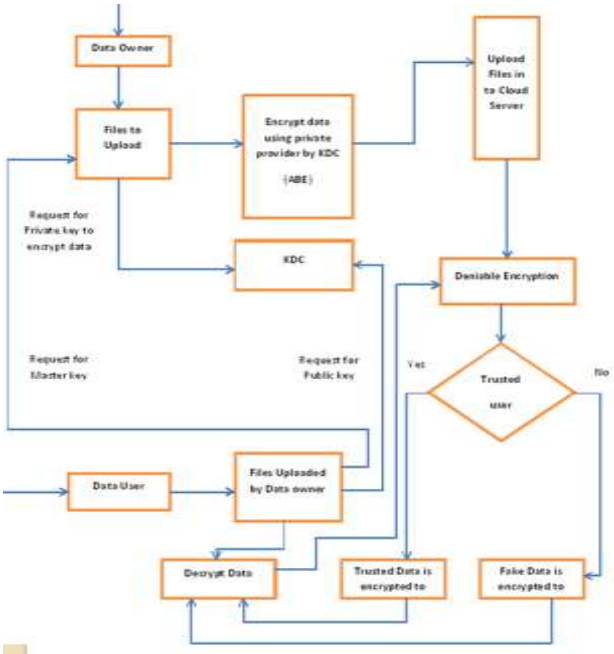

Fig 1. System Architecture

CONCLUSION

In this work, I proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. The proposed scheme provides a possible way to fight against immoral interference with the right of privacy. I hope more schemes can be created to protect cloud user privacy.

REFERENCES

1. V. 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.

2. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.
3. S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public Key Cryptography*, 2013, pp. 162–179.
4. A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Crypto*, 2012, pp. 199–217.
5. S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public Key Cryptography*, 2013, pp. 162–179.
6. P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds." *IEEE T. Cloud Computing*, pp. 172–186, 2013.
7. P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in *WPES*, 2010, pp. 31–42.
8. M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption," in *SOFSEM*, 2008, pp. 599–609.
9. M. H. Ibrahim, "A method for obtaining deniable public-key encryption," *I. J. Network Security*, vol. 8, no. 1, pp. 1–9, 2009.
10. J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in *Crypto*, 2002, pp. 111–126.