International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

AUDIT FREE CLOUD via DENIABLE ATTRIBUTE BASED ENCRYPTION

Kavitha S, Kousalya G, Lavanya C, Ms. P. Kavitha

Assistant Professor, Department of Computer Science and Engineering, RMK Engineering College, Tamilnadu, India

---

Abstract – *The need of cloud storage services have become extremely necessary in the recent days.. Due to the insistance on data security, many cloud storage encryption schemes have been schemed to protect data from those who do not have the right access. Users believed these schemes prevented the access from hackers; however, in practice, some authorities may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this work, we present our framework for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake data to protect the user information. Since coercers will not be able to predict whether the obtained data true or fake, the cloud storage providers ensure that user privacy is still securely protected.*

Key Words: Cloud Storage, Encryption Schemes, Coercers, Cloud-storage Providers.

1. INTRODUCTION

A large collection of systems connected in private or public networks which provides dynamic infrastructure for data, application and file storage is termed as a cloud computing. It is a practical approach to transform a data center from a capital- intensive set up to a variable priced environment. The reality of large volumes of data storage and maintenance is offered with a massive infrastructure by the cloud providers. Since the cloud can scale dynamically, sudden workload spikes can also be managed effectively and efficiently. The deliver speed is critical due to enterprises having to adapt, even more rapidly, to changing business conditions. Using the most appropriate building blocks necessary for deployment, cloud computing stresses on getting applications to market very quickly. The crucial element that warrants security is data security. From vendors, enterprises are often reluctant to buy an assurance of business data security. Lose of data to competition and the data confidentiality of consumers are their major fears. Due to various security concerns, the actual storage location is not disclosed in many instances. The interface between service suppliers and multiple groups of service consumers, is the way in which the interface action moves with respect to cloud computing.

2. EXISTING SYSTEM

2.1. Key Policy Attribute Based Encryption:

1.User setup: A parameter K is taken as the input and it returns the public key PK and a system master key MK. The message senders use the PK for encryption. MK which is kept secret by the authority is used to generate user secret keys.
2.Encryption: This algorithm takes a message M, the Public key PK, and a set of specific attributes as the input. The output is the ciphertext E.
3.Key Generation: This algorithm takes an access structure T and the master secret key MK as the input The outputs is a secret key SK which helps the user to decrypt a message that is encrypted only if a set of attributes equals T.
4.Decryption: It takes as input the user's secret key SK for Access structure T and the ciphertext E, which was encrypted under the attribute set. It outputs the message M if and only if the attribute set satisfies the user's access structure T.

2.2 Ciphertext-Policy Attribute-Based Encryption:

1.cpabe-setup: This program generates the public key and master keys.
2.cpabe-keygen: This program allows the user to produce private keys associated with a set of attributes. It is critical that the user keep this key private.
3.cpabe-enc: This program encrypts a message using a public key and a set of attributes.
4.cpabe-dec: This program decrypts an encrypted message using the encrypting user's public key, and the decrypting user's private key. The decrypted file will share the name with the encrypted file.

3. PROPOSED METHODOLOGY AND DISCUSSION

3.1. Deniable Encryption:

When hackers or coercers try to interpret the private data of the senders and the receivers, the deniable encryption creates a convincing fake evidence of forged data in ciphertexts to satisfy them. This will result in making the coercer's efforts useless. Since the coercers are not aware of the original data, they will not be able whether they have received the original data or not. By this methodology, we can provide audit-free cloud storage

services. The data owners who store their data on the cloud are like senders and those who can access the encrypted data plays the receiver role in the deniable encryption scheme. This also includes the cloud storage providers themselves, who have system wide secrets and can be able to decrypt all encrypted data.

3.2. Composite Order Bilinear Group:

A composite order group is a 2-dimensional vector space, More concretely in the context of a bilinear map, if gg is a generator with order N=pqN=pq, then gp=gqgp=gq generates an order-pp subgroup, and gq=gpgq=gp generates an orderqq, and e(gp,gq)=1e(gp,gq)=1. They cancel each other out, and so you can think of {gq,gp}{gq,gp} as an orthogonal basis for the a 2-dimensional vector space.The way this is typically used is that the bilinear "functionality" of a scheme is carried out in one dimension (e.g., in the exponent of gpgp) while the other dimension (e.g., the exponent of gqgq) is used for "blinding". Orthogonality ensures that the blinding factors just disappear after the bilinear map. A framework have been developed for cryptographic constructions using prime-order bilinear groups (called dual-pairing vector spaces, DPVS). It is a nice abstraction that allows you to build (from primeorder groups) nn-dimensional orthogonal vector spaces that have a suitable pairing. It's like having the above effect, but now even with of a product of nn primes! I think most people in the field believe that prime-order constructions can be "ported" to prime-order groups, using these DPVS techniques.

3.3. Attribute-Based Encryption:

Using cloud storage services, we can store and access data from anywhere. The data security features protects the data and information and prevents the access by other users. Among various encryption schemes, Attribute Based Encryption is proposed to be the most efficient scheme. In many schemes, third party authorities are involved in transferring the data between the sender and the receivers which may result in coercers compelling the authorities to reveal the data. This is because, here the encrypted data and so they are requested to provide the data. In 2010,when FBI forced Google to release specific information, it released the documents without notifying its users. The effectiveness of the data will be lost once the cloud storage providers are compromised.

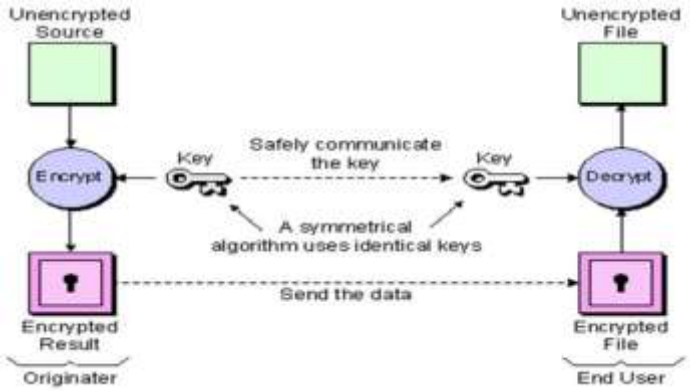
4. IMPLEMENTATION OF MODULES

The proposed scheme consists of four algorithms which is defined as follows:

1.Setup:
The inputs taken by the algorithm are security parameters and attribute universe of cardinality N. A bilinear group of prime numbers are defined. It outputs a public key and the master key which is known only to the authority party.
2.Encryption:
The inputs taken by the algorithm are message, public key and a set of attributes. The output is a cipher text.
3.Key Generation:
The algorithm takes an access tree, master key and public key as inputs. The output is a user secret key.
4.Decryption:
Inputs are cipher text, user secret key and public key. It first computes a key for each leaf node. Then, aggregates the results using polynomial interpolation technique and returns the message.

5. ALGORITHM AND ARCHITECTURE

The scheme is composed of the following algorithms:
1] Setup(1) → (PP,MSK): This algorithm takes security parameter as input and returns public parameter PP and system master key MSK.
2] KeyGen(MSK, S) → SK: Given set of attributes S and MSK, this algorithm outputs private key SK.
3] Enc(PP,M,A) → C: This encryption algorithm takes as input public parameter PP, message M, and LSSS access structure A = (M,) over the universe of attributes. It encrypts M and outputs a ciphertext C, which can be decrypted by only those who provide an attribute set that satisfies the access structure A.
4] Dec(PP, SK,C) → {M, }: This decryption algorithm takes as input public parameter PP, private key SK with its attribute set S, and ciphertext C with its access structure A. If S satisfies A, then this algorithm returns M; otherwise, this algorithm returns .
5] OpenEnc(PP,C,M) → PE: This algorithm is for the sender to release encryption proof PE for (M,C).OpenDec(PP, SK,C,M) → PD: This algorithm is for the receiver to release decryption proof PD for (M,C).
6] Verify(PP,C,M, PE, PD) → {T, F}: This algorithm is used to verify the correctness of
PE and PD



6. CONCLUSION

Thus, a deniable CP-ABE scheme has been framed to build an audit-free cloud storage service. The deniability feature prevents coercion and ensures secure cloud data sharing with a fine-grained access control mechanism. It enables the most efficient way to fight against coercion with the private information. In this project, we proposed a deniable CPABE scheme to provide an audit-free cloud storage service. In future, more enhanced schemes may be structured to improvise the cloud storage services.

REFERENCES

1) Changji Wang1,2,3 and Jianfa Luo1,2 "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 810969.

2) Guojun Wang, Qin Liu, Jie Wu "Hierarchical Attribute-Based Encryption for FineGrained Access Control in Cloud Storage Services" CCS'10, October 4–8, 2010, Chicago, Illinois, USA. ACM 978-1-4503-0244-9/10/10.

3) S. Gokuldev, S.Leelavathi "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013.

4) M. H. Ibrahim, "A method for obtaining deniable public-key encryption," I. J. Network Security, vol. 8, no. 1, pp. 1–9, 2009.

5) J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in Crypto,2002, pp. 111–126.

6) R. Bendlin, J. B. Nielsen, P. S. Nordholt, and C. Orlandi, "Lower and upper bounds for deniable public-key encryption," Cryptology ePrint Archive, Report 2011/046, 2011, http://eprint.iacr.org/.

7) D.M Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in Eurocrypt,2010, pp. 44–61.

8) A.B. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in Eurocrypt, 2012,pp. 318–335.

9) A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of technology, 1996.

10) D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in TCC, 2005, pp. 325–341.

11) H. Krawczyk and T. Rabin, "Chameleon signatures," in NDSS, 2000.

12) D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in Eurocrypt, 2006, pp. 573–592.