Audit Free Cloud Storage through Encryption Function Based Deniable

[1]POTHURAJU JANGAIAH [2]K BIKSHAPATI

[1] PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

[2]Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206

ABSTRACT— 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.

1 INTRODUCTION

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. 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 eemingly more and more difficult.

2 PRELIMINARIES

2.1 Prime Order Bilinear Groups

Let G and GT be two multiplicative cyclic groups of prime order p, with map function e : G × G → GT . Let g be a generator of GG. G is a bilinear map group if G and e have the following properties:

- Bilinearity: ∀u, v ∈ G and a, b ∈ Z, e(ua, vb) = e(u, v)ab.
- Non-degeneracy: e(g, g) 6= 1.
- Computability: the group action in G and map function e can be computed efficiently.

2.2 Waters CP-ABE

In this subsection, we provide an introduction to Waters CP-ABE [4]. Waters used LSSS to build an access control mechanism. Here, we first review the definition of LSSS.

Definition 1 (LSSS: Linear Secret Sharing Schemes [24]):

A secret sharing scheme _ over set of parties P is called linear (over Zp) ifAccording to the above definition, an LSSS scheme has

the linear reconstruction property. That is, given LSSS, access structure A, and valid shares of a secret s, s can be recovered by those who have authorized sets. In [24], Beimel shows that the recovery procedure is time polynomial in the size of M. In an ABE scheme, parties represent attributes. The Waters CP-ABE scheme is composed of the following algorithms:

- **Setup**() → (MSK, PK): This algorithm chooses a bilinear group of prime order p with generator g,

random elements _, a ∈ Zp, and hash function H : {0, 1}∗ → G. The public key PK is {g, e(g, g)_, ga} and the system secret key MSK is g_.

- **Encrypt**(PK, (M, _),M) → CT : Given message M and LSSS access structure (M, _), this algorithm first chooses a random vector −→v = (s, y2, . . . , yn) ∈ Znp . Let M be a l × n matrix and Mi denote the ith row of M. This algorithm calculates _i = −→v Mi, ∀i ∈ {1, . . . , l}. Further, this algorithm chooses r1, . . . , rl ∈ Zp. The output ciphertext will bee(g, g)_s, gs, (ga_1H(_(1))−r1 , gr1), . . . , (ga_lH(_(l))−rl , grl)} = {C,C′, (C1,D1), . . . , (Cl,Dl)},

with a description of (M, _).

- **KeyGen**(MSK, S) → SK: Given set S of attributes, this algorithm chooses t ∈ Zp randomly and outputs the private key as:

K = g_+at,L = gt, ∀x ∈ SKx = H(x)t.

- **Decrypt**(CT, SK) →M: Suppose that S satisfies the access structure and let I ⊂ {1, . . . , l} be defined as I = {i : _(i) ∈ S}. This algorithm finds a set of constants {wi ∈ Zp} such that P i∈I wi_i = s. The decryption algorithm computes e(C′,K)/(Y i∈I (e(Ci,L)e(Di,K_(i)))wi) = e(g, g)_s and derives M from the ciphertext. The security of Waters CP-ABE scheme is based on the decisional q-parallel bilinear BDHE

assumption, which is defined as follows:

Definition 2 (Decisional q*-parallel BDHE Assumption):*

Let a, s, b1, . . . , bq

R ←− Z

p

and g

be a

generator of G.

Given

D :=

gs·bj , ga/bj , . . . , g(aq/bj),

g(aq+2/bj), . . . , g(a2q/bj)

∀1≤j,k≤q,k6=j ga·s·bk/bj , . . . , gaq·s·bk/bj

and element T ∈ GT , we assume that for any PPT algorithm A that outputs in {0, 1},

AdvA := |P[A(D, e(g, g)aq+1s) = 1] − P[A(D, T) = 1]| is negligible.

Theorem 1: Suppose the decisional q-parallel BDHE assumption holds, then no polynomial time adversary can selectively break the Waters CP-ABE system in the CPA-model.

The proof can be f**2.3 Composite Order Bilinear Groups**

The composite order bilinear group was first introduced in [25]; we use it to construct our scheme. Here we provide a brief introduction. Let G and GT be two multiplicative cyclic groups of composite order N = p1p2 . . . pm, where p1, p2, . . . , pm are distinct primes, with bilinear map function e : G × G → GT . For each

prime pi, G has a subgroup Gpi of order pi. We let g1, g2, . . . , gm be the generators of these subgroups respectively. Each element in G can be expressed in the form of ga1 1 ga2 2 . . . gam m , where a1, a2, . . . , am ∈ ZN. If ai is congruent to zero modulo pi, we say that this element has no Gpi component.We say an element is in Q i∈S Gpi , where S is a subset from 1 . . .m, if ∀i ∈ S, ai is not congruent to zero modulo pi

3.DEFINITION

3.1 Deniable CP-ABE Scheme

Deniable encryption schemes may have different properties and we provide an introduction to many of these properties below.

- *ad hoc deniability vs. plan-ahead deniability*: The former can generate a fake message (from the entire message space) when coerced, whereas the latter requires a predetermined fakemessage for encryption. Undoubtedly, all bitwise encryption schemes are ad hoc.

- *sender-, receiver-, and bi-deniability*: The prefix here in each case implies the role that can fool the coercer with convincing fake evidence. In sender-deniable encryption schemes and receiver-deniable schemes,

it is assumed that the other entity cannot be coerced. Bi-deniability means both sender and receiver can generate fake evidence to pass third-party coercion.

- *full deniability vs. multi-distributional deniability*: A fully deniable encryption scheme is one in which there is only one set of algorithms, i.e., a keygeneration algorithm, an encryption algorithm and so on. Senders, receivers and coercers know this set of algorithms and a sender and a receiver can fool a coercer under this condition. 3.1.1 Is a Confidential PK Practical? In the above definition, our scheme assumes that PK will be kept secret from the coercer. Some may argue that it is impractical, stating that coercers can pretend to be users in cloud storage services and obtain the PK. Once the PK is released to coercers, they can easily generate deniably encrypted ciphertexts and use these ciphertexts to determine the types of receiver proofs. To address this question, we must return to the basic assumption of deniable encryption schemes, i.e., **senders and receivers want to hide their communication messages from outside coercers**. Like all other cryptographic schemes, secrets must be assumed to be unknown to adversaries and our scheme is no exception. Therefore assuming that the PK is kept secret to coercers is acceptable and unavoidable.

4. SECURITY PROOF

To prove that our deniable encryption scheme is secure requires this scheme to be a valid encryption scheme. For a multi-distributional deniable encryption scheme,

it is only necessary to prove the security from the normal algorithm set. That is, we only need to prove the security of a scheme composed of the following four algorithms **Setup**, **KeyGen**, **Enc**, and **Dec**. As for the deniable algorithms, since deniable keys and ciphertexts are indistinguishable from normal keys and ciphertexts, which will be proved in the next subsection, deniable algorithms will be treated as normal algorithms which are proved to be secure. In other words, if the normal algorithm set can form a secure scheme, but the deniable set cannot, the security test will be a tool to distinguish these two sets of algorithms and there will be no deniability in our scheme. For proving security, we will reduce Waters CP-ABE to our deniable ABE scheme.

4.1 Deniability Proof

To prove the deniability of our CP-ABE scheme, we must show (M,C, PE, PD) and (M′,C′, P′ E, P′ D) are indistinguishable. Since M,C,PE,PD are pairwise independent because of the security property, we need only show the indistinguishability between C and C′, PE and P′ E , and PD and P′ D .

5.PERFORMANCE EVALUATION

In this section, we evaluate the performance of our idea by implementing two deniable schemes: the composite order scheme and the prime order simulation scheme. We compare them with the Waters scheme [4]. We use the Pairing Based Cryptography (PBC) library for cryptographic operations. We use type A1 pairing because this type of pairing can support both prime order and composite order groups. In our experiment, we set the size of each prime to 512 bits, which is equal to 256 bits of security [32]. Under this setting, the composite group order size is 1536 bits. However, when considering security, the composite order scheme with a group size of 1536 bits is equal to the prime order scheme with a group size of 512 bits. This is because a message is encrypted in one subgroup whose group size is 512 bits. Our experiments focus on encryption and decryption performance. The **Setup** and **KeyGen** performance are skipped because these two algorithms are not time critical. The four **Open** algorithms are low-cost algorithms. because these algorithms only return existing information.

The cost of **Verify** algorithm is equal to that of **Dec**. Note that we do not distinguish deniable encryption from normal encryption; their numbers of arithmetic operations and pairing operations are equal, and therefore the normal one and the deniable one will have similar performance. In our design, the encryption cost and the decryption cost depend on required attribute numbers. For convenience, we make all attributes mandatory as our cryptographic policy. We run the experiments with different attribute numbers, from 10 to 1000. Our experiments focus on one block encryption/decryption. Each block is set to 128 bytes because PBC reads around 130 bytes to generate a GT element when the group size is 512 bits5. A large file can be divided into multiple blocks, and all blocks can be protected by one secret s. Because GT multiplication and H are lightweight operations, we use one-block encryption/decryption to evaluate the performance. The experiments are tested on a virtual machine with 3.47 GHz CPU and 8 GB memory. As we can see, encryption time and decryption time grow linearly over the attribute number in all three schemes.

6.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

7. 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.

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.

8.IMPLEMENTATION

Data Owner In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud.

Cloud Server The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers.

Key Distribution centre KDC who is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

9 CONCLUSION

In this work, we 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. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy.

10 REFERENCES

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

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conferenceon Computer and Communications Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[4]B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, 2011, pp. 53–70.

[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.

[6]S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.

[7]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.

[8] Wired. (20 4) Spam suspect uses google docs; fbi happy. [Online].Available: http://www.wired.com/2010/04/cloud-warrant/

[9] Wikipedia. (2014) Global surveillance disclosures (2013present). [Online].Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)

[10](2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden

[11] (2014) Lavabit. [Online]. Available: http://en.wikipedia. org/wiki/Lavabit

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

[13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Eurocrypt, 2010,pp. 62–91.

[14]N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R`afols, “Attribute-based encryption chemes with constant-size ciphertexts,” Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.

[15]M. D¨urmuth and D. M. Freeman, “Deniable encryption with negligible detection probability: An interactive construction,” inEurocrypt, 2011, pp. 610–626.

[16]A. O’Neill, C. Peikert, and B. Waters, “Bi-deniable public-key encryption,” in Crypto, 2011, pp. 525–542.

AUTHOR’S PROFILE:

POTHURAJU JANGAIAH

PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education,
Ramapuram (kattakommu Gudem),
Chilkur(M), Kodad, Telangana 508206.

K BIKSHAPATI

Assistant Professor, Department Of CSE.
Gandhi Academy Of Technical Education,
Ramapuram (kattakommu Gudem),
Chilkur(M), Kodad, Telangana 508206