SECURE CLOUD STORAGE USING DENIABLE ATTRIBUTE BASED ENCRYPTION

S. Muthuselvi and P.Jeyadurga

Assistant Professor, Computer Science and Engineering,
Dr. SivanthiAditanar College of Engineering, Tiruchendur, India

ABSTRACT

Cloud storage services are a lot of well-liked today . To secure information from those that don't have access, several encoding schemes are projected. Most of the projected schemes assume cloud storage service suppliers or trustworthy third parties handling key management are trustworthy and can't be hacked; but, in follow, some entities could intercept communications between users and cloud storage suppliers and so compel storage suppliers to unleash user secrets by victimisation government power or alternative means that. During this case, encrypted information are assumed to be identified and storage suppliers are requested to unleash user secrets. Since it's tough to fight against outside coercion, we tend to aimed to create Associate in Nursing encoding theme that might facilitate cloud storage suppliers avoid this plight. We provide cloud storage suppliers means that to make pretend user secrets. Given such pretend user secrets, outside coercers will solely obtained solid information from a user's keep cipher text. Once coercers suppose the received secrets are real, they'll be happy and a lot of significantly cloud storage suppliers won't have discovered any real secrets. Therefore, user privacy continues to be protected.

KEYWORDS

Deniable Encryption, Composite Order Bilinear Group, Attribute Based Encryption, Cloud Storage.

1. INTRODUCTION

Cloud storage services have chop-chop become progressively popular. Users will store their information on the cloud and access their information anyplace at any time. Because of user privacy, the information keep on the cloud is often encrypted and guarded from access by alternative users. The cooperative property of the cloud information, attribute based cryptography (ABE) is considered one of the most appropriate cryptography schemes for cloud storage. There are various ABE schemes that are projected, including [1], [2], [3], [4], [5], [6], [7]. Most of the projected schemes assume cloud storage service suppliers or trustworthy third parties handling key management are trustworthy and can't be hacked; but, in follow, some entities might intercept communications between users and cloud storages suppliers so compel storage suppliers to unleash user secrets by mistreatment government power or alternative means during the case encrypted information are assumed to be celebrated and storage providers are requested to unleash user secrets. As an example, in 2010, while not notifying its users, Google free user documents to the FBI when receiving a hunt warrant [8]. In 2013, Edward Snowden disclosed the existence of global police work programs that collect such cloud information as emails, texts, and voice messages from some technology firms [9], [10]. Once cloud storage providers are compromised, all cryptography schemes lose their effectiveness. Those we have a tendency to hope cloud storage providers will fight against such entities to take care of user privacy through legal avenues, it's ostensibly a lot of and more troublesome.

As one example, Lavabit was AN email service company that protected all user emails from outside coercion; sadly, it failing and set to shut down its email service [11].Since it's troublesome to fight against outside coercion, we aimed to create AN encoding theme that would facilitate cloud storage suppliers avoid this difficulty. In our approach, we provide cloud storage suppliers means that to create faux user secrets. Given such faux user secrets, outside coercers will solely obtained solid knowledge from a user's hold on cipher text. Once coercers suppose the received secrets square measure real, they're going to be happy and additional significantly cloud storage suppliers won't have unconcealed any real secrets. Therefore, user privacy remains protected. This concept comes from a special reasonably encoding scheme known as disavowable encoding, initial planned in [12]. disavowable encoding involves senders and receivers creating convincing faux proof of solid knowledge in cipher texts such outside coercers square measure happy. This method tries to altogether block coercion efforts since coercers understand that their efforts are useless. We make use of this idea such cloud storage suppliers will provide audit-free storage services. With in the cloud storage scenario, knowledge house owners World Health Organization store their knowledge on the cloud are similar to senders within the disavowable encoding theme. Those who will access the encrypted information play the role of receiver within the confutative cryptography theme, as well as thecloud storage suppliers themselves, United Nations agency have system wide secrets and should be able to rewrite all encrypted data.

In this work, we have a tendency to describe a confutative ABE theme for cloud storage services. we have a tendency to build use of ABE characteristics for securing keep information with a fine-grained access control mechanism and confutative cryptography to stop outside auditing. Our theme relies on Waters cipher text policy-attribute based mostly cryptography (CP-ABE) theme [4]. We have a tendency to enhance the Waters theme from prime order bilinear teams to Composite order additive teams. **Waters cipher text policy-attribute based encryption (CP-ABE)** Strategies encoded information can be kept classified regardless of whether the capacity worker is untrusted; in addition, in this techniques are secure against agreement assaults. Past characteristic based encryption frameworks utilized ascribes to depict the scrambled information and incorporated strategies into client's keys; while in this framework credits are utilized to portray a client's certifications, and a gathering encoding information decides an arrangement for who can decode. Subsequently, in this techniques are adroitly nearer to conventional access control strategies, for example, job based admittance control (RBAC). Also, we give an execution of this framework and give execution estimations. By the subgroup call downside assumption, our scheme enables users to be able to give pretend secrets that appear legitimate to outside coercers. In this attribute based encryption method the secrets information does not know the outsider. Call downside assumption is used to predict the secrets information from outsiders if suppose the outsiders hack the information means the call downside assumption will sent a wrong information to the outsiders.

2. RELATED WORK

Markus Durmuth, David Mandell Freeman [2011] proposed the first sender-deniable public key encryption system with a single encryption algorithm and negligible detection probability. It describes a generic interactive construction based on a public key bit encryption scheme. Sender–deniable public key encryption system use a public key bit encryption scheme that admits an "oblivious cipher text generation" algorithm, which allows a public key holder to sample a cipher text that is distributed as an encryption of a random bit. To encrypt a bit b ϵ (0, 1), we first obtain 4n + 1 public keys for the underlying encryption scheme. We construct n + 1 encryptions of b, construct n encryptions of 1 - b, and sample 2n cipher texts obliviously, each under a different public key, and then permute the output randomly. Decrypting all cipher texts individually and

taking the majority recovers the original message with noticeable probability. Repeating the protocol multiple times in parallel reduces the decryption error. Adam O'Neill, Chris Peikert, Brent Waters [2011] proposed bi-deniable public-key cryptosystems, in which both the sender and receiver can simultaneously equivocate. They stress that the schemes are non-interactive and involve no third parties. One of the systems is based generically on "simulatable encryption" as while the other is lattice-based and with techniques that may be of independent interest. Both schemes work in the "multi-distributional" model, in which the parties run alternative key-generation and encryption algorithms for equivocable communication, but claim under coercion to have run the prescribed algorithms. Although multi-distributional deniability has not attracted much attention, they argue that it is meaningful and useful because it provides credible coercion resistance in certain settings, and suffices for all of the related properties. Paolo Gasti, Giuseppe Ateniese, Marina Blanton [2010] proposed sender-and-receiver deniable public-key encryption scheme that is both practical and is built from standard tools. To construct a sender-deniable plan-ahead public key encryption scheme using RSA-OAEP and the Damgard-Jurik generalization of Paillier's encryption scheme as building blocks. Then extend it to provide non-interactive sender-and-receiver deniable plan-ahead public-key encryption. Finally, we show how to efficiently construct a public key deniable encryption scheme using any IND-CPA encryption scheme as a black box. It provide a high throughput (i.e., linear in the size of the ciphertext) for messages that can be deniably communicated. Amit Sahai and Brent Waters [2005] proposes a fuzzy IBE scheme allows for private key for an identity, to decrypt a ciphertext encrypted with an identity. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity.

3. ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country in which they live, or the kind of subscription they have). Attribute based encryption (ABE) more appropriate for access control to information put away in the cloud. For this reason, we focus on providing for the encryptor full power over the entrance rights, giving possible key administration even in the event of different autonomous specialists, and empowering suitable client denial, which is fundamental practically speaking.

Use of ABE characteristics for securing keep information with a fine-grained access control mechanismFine-grained access control frameworks encourage giving differential access rights to a bunch of clients and permit adaptability in determining the entrance rights of individual clients.
Usage of Attribute based encryption (ABE) can be utilized for log encryption. Rather than encoding each piece of a log with the keys, everything being equal, it is conceivable to scramble the log just with ascribes which coordinate beneficiaries' credits.

3.1. Proposed Method

My plan-ahead, bideniable, and multi-distributional CP-ABE scheme is composed of the following algorithms:

- **Setup** (1) → (PP, MSK): This algorithm takes security parameter as input and returns public parameter PP and system master key MSK.

- **KeyGen** (MSK, S) → SK: Given set of attributes S and MSK, this algorithm outputs private key SK.
- **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. This algorithm encrypts M and outputs a cipher text C, which can be decrypted by those who possess an attribute set that satisfies access structure A. Note that A is contained in C.

- **Dec** (PP, SK,C) → {M,⊥}: This decryption algorithm takes as input public parameter PP, private key SK with its attribute set S, and cipher text C with its access structure A. If S satisfies A, then this algorithm returns M.

- **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).

- **Verify** (PP,C,M, PE, PD) → {T, F}: This algorithm is used to verify the correctness of PE and PD.

- **DenSetup**(1) → (PP,MSK, PK): This algorithm takes security parameter as input and returns public parameters PP, system master key MSK, and system public key PK. PK is known by all system users and is kept secret to outsiders.

- **DenKeyGen**(MSK, S) → (SK, FK): Given set of attributes S and MSK, this algorithm outputs privatekey SK as well as FK for the user, where FK will be used for generating fake proof later.

- **DenEnc**(PP, PK,M,M′,A) → C′: Aside from the inputs of the normal encryption algorithm, this deniable encryption algorithm needs public key PK and fake message M′. The output cipher text must be indistinguishable from the output of **Enc**.

- **DenOpenEnc**(PP,C′,M′) → P′ E : This algorithm is for the sender to release encryption proof P′ E for fake message M′. The output must be indistinguishable from the result of **OpenEnc** and must pass the **Verify** algorithm.

- **DenOpenDec**(PP, SK, FK,C′,M′) → P′ D: This algorithm is for the receiver to release decryption proof P′D for fake message M′. The output must be indistinguishable from the result of **OpenDec** and must pass the **Verify** algorithm.

We require the following properties:

1) **Security**: The tuple {**Setup**,**KeyGen**, **Enc**,**Dec**} must form a secure CP-ABE scheme in a security model. In this work, we propose a CPA secure scheme and a CCA secure scheme. These two security models are defined in Section 3.2.

2) **Bi-deniability**: The CP-ABE is bi-deniable if, given public parameter PP, the two distribution tuples (M,C, PE, PD) and (M′,C′, P′ E , P′ D) are computational indistinguishable, where M,M′ are claimed messages, C,C′ are normally and deniably encrypted cipher texts, respectively, and PE, PD, P′ E , P′ D are proofs generated from the

normal and deniable open algorithms, respectively. That is, there is no PPT algorithm A for which

Adv A := |P[A(PP, (M,C, PE, PD)) = 1] − P[A(PP, (M′,C′, P′E , P′D)) = 1] |is non-negligible.

3) **Deniable Receiver Proof Consistency**: The deniable CP-ABE is deniable receiver proof consistent if a deniable receiver proof is convincing even when considering all cipher texts in the system. That is, given set of cipher texts C, including normally encrypted cipher texts and deniably encrypted cipher texts, normal proof PD and deniable proof P′D , there is no PPT algorithm A for which

Adv A := |P[A(C, PD) = 1]− P[A(C, P′D) = 1]|
is non-negligible.

We note that the last requirement is unusual for deniable encryption schemes. We build our scheme with this requirement for practicality. In a cloud storage service.

4. RESULTS AND DISCUSSIONS

Fig:4.1 Registration

Fig4.1 illustrate the process of registration of users to access the cloud storage services. The details of the users who are all registrated for stored in database sql.

Fig:4. 2login

The registrated user login into the cloud is illustrated in fig 4.2.

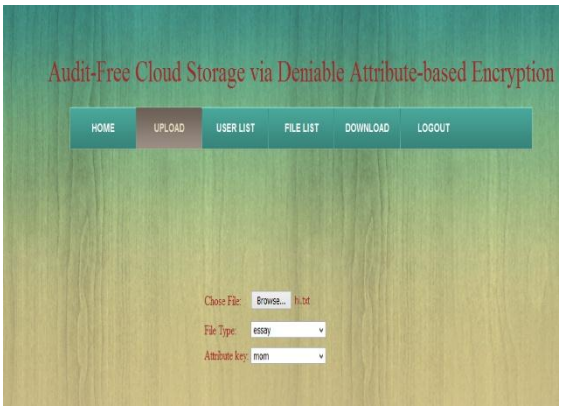

Fig 4.3.uploading a file

Fig 4.3 illustrate the process of uploading the file of the user into to the cloud environment.

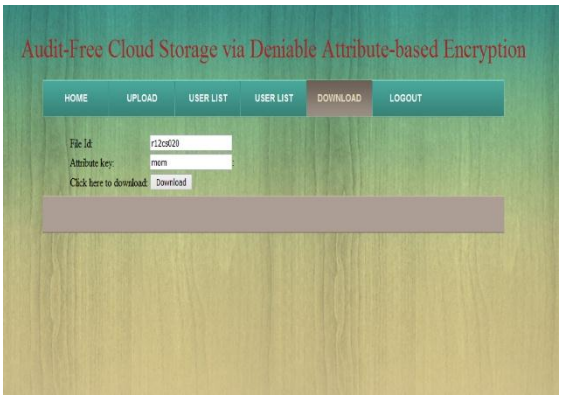

Fig:4.4 download the file

Fig 4.4 illustrate the process of download the file if the user needs to access the file.

Fig:4.5 Authenticate user login

Fig4. 5 illustrate the process of login of the authenticated user.

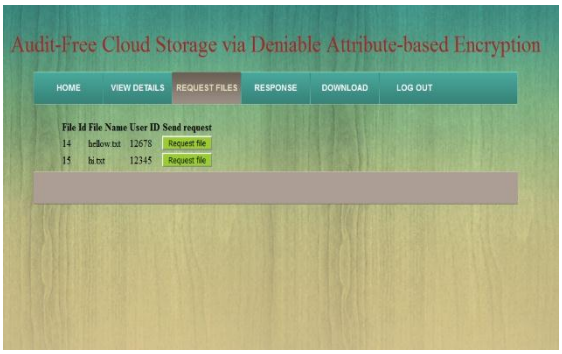

Fig:4.6 Request file

Fig4.6 illustrate the process of authenticated user to request to provider to download the file of the particular user. Then the provider give the response to download the file.

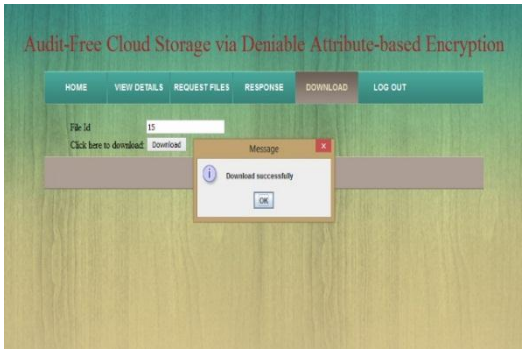

Fig:4.7 Download

Fig4.7 illustrate the process of downloading the file of the user.

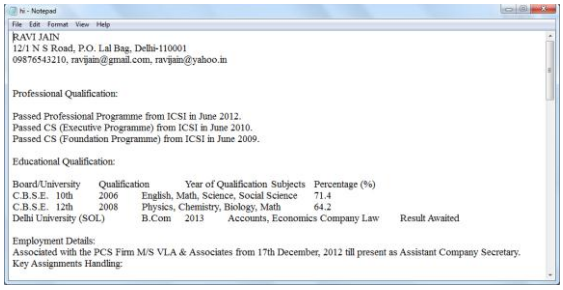

Fig:4.8 Downloaded file

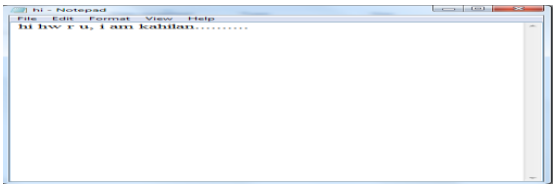

Fig:4.9 Original file

Fig4.8 and fig4. 9 shows the difference between the original file and the downloaded file

5. CONCLUSION

In this work we proposed a deniable CP-ABE with CCA and CPA to build audit free cloud storage services. To protect the user secret from the coercers and the attackers deniable CP-ABE is used. 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.

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 Conference on 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 andPrivacy, 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. (2014) 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/Globalsurveillance 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. Rafols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor.Comput. Sci., vol.422, pp. 15–38, 2012.

[15] M. Durmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626.

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

[17] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, 2010, pp. 31–42.

[18] M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption," in SOFSEM, 2008, pp. 599–609.