IJSEAT International Journal of Science Engineering and Advance Technology

A Deniable Cp-Abe Scheme For An Audit-Free Cloud Storage Service

[1]P.Aparna, [2]K.Satya Narayana Murthy
[1,2,]Dept. of CSE, Baba Institute Of Technology & Sciences,
Bakkannapalem, Madhurawada,
Visakhapatnam ,AP, India

ABSTRACT:

To brawl against outside coercion, we meant to build an encryption scheme that could help cloud storage providers keep away from this quandary. In our move toward, we present cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only get hold of phony data from a user's stored cipher text. Once coercers imagine the received secrets are genuine, they will be content and more prominently cloud storage providers will not have exposed any real secrets. Consequently, user isolation is still protected. This concept comes from a special kind of encryption scheme called deniable encryption. Deniable encryption absorb senders and receivers form convincing fake evidence of forged data in cipher texts such that outside coercers are contented.

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

1] INTRODUCTION:

For a new cloud storage encryption scheme that allow cloud storage providers to make convincing fake user secrets to defend user privacy. Since coercers cannot tell if get hold of secrets are true or not, the cloud storage providers make certain that user privacy is still firmly protected. Cloud storage services have quickly turn into more and more well-liked. Users can store their data on the cloud and right of entry their data anywhere at any time. Since of user privacy, the data stored on the cloud is classically encrypted and secluded from access by other users. Bearing in mind the joint property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most appropriate encryption schemes for cloud storage.

2] LITERATURE SURVEY:

2.1] THE AUTHOR, B. Waters **(ET .AL), AIM** we display two developments of Fuzzy IBE plans. Our developments can be seen as an Identity-Based Encryption of a message under a few traits that form a (fuzzy) identity. Our IBE plans are both error tolerant and secure against intrigue attacks. Furthermore, our fundamental development does not utilize random oracles. We demonstrate the security of our plans under the Selective-ID security show.

2.2] THE AUTHOR, O. Pandey **(ET .AL), AIM** We build up another cryptosystem for fine-grained sharing of encrypted information that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are named with sets of traits and private keys are connected with get to structures that control which cipher texts a client can decrypt. We show the appropriateness of our development to sharing of review log data and communicate encryption. Our development underpins appointment of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

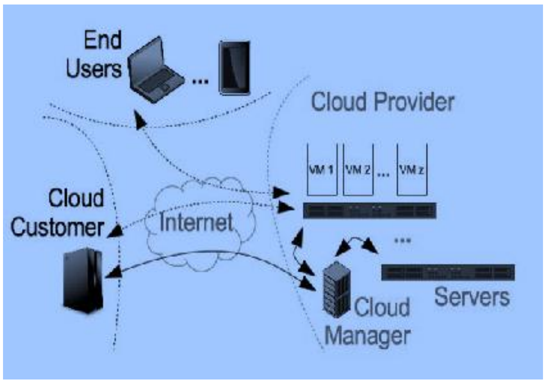
3] PROBLEM DEFINITION:

Like usual encryption schemes, deniable encryption can be alienated into a deniable shared key scheme and a public key scheme. Bearing in mind the cloud storage scenario, we center our efforts on the deniable public key encryption scheme. When sending an encrypted bit, the sender will send a set of encrypted data which may be usually encryptedor unaware. Consequently, the sender can claim some sent messages are oblivious while in fact they are not. The design can be applied to the receiver side such that the scheme is a bi-deniable scheme.

4] PROPOSED APPROACH:

We explain a deniable ABE scheme for cloud storage services. We create ABE characteristics for protected stored data with a fine-grained access control mechanism and deniable encryption to put off outside auditing. Our method is based on Waters cipher text policy-attribute based encryption (CP-ABE) scheme. We augment the Waters scheme from main order bilinear groups to complex order bilinear groups. By the subgroup decision problem statement, our scheme facilitate users to be talented to supply fake secrets that seem genuine to outside coercers.

5] SYSTEM ARCHITECTURE:



6] PROPOSED CONSTRUCTION:

6.1] AD HOC DENIABILITY VS. PLAN-AHEAD DENIABILITY:

The formercan produce a fake message from the entiremessage space when coerced, while the latter requiresa prearranged fakemessage for encryption.Unquestionably, all bitwise encryption schemes are adhoc.

6.2] SENDER-, RECEIVER-, AND BI-DENIABILITY:

The prefix here ineach case involves the position that can fool the coercerwith persuasivecounterfeit evidence. In sender-deniableencryption schemes and receiver-deniable schemes,it is unspecified that the other thing cannot be coerced.Bi-deniability means both sender and receiver canproducecounterfeitconfirmation to pass third-party coercion.

6.3] FULL DENIABILITY VS. MULTI-DISTRIBUTIONAL DENIABILITY:

Acompletely deniable encryption method is one in whichthere is only one set of algorithms, i.e., a keygenerationalgorithm, an encryption algorithm andso on. Senders, receivers and coercers be acquainted with thisset of algorithms and a sender and a receiver canhoodwink a coercer under this situation.

6.4] INTERACTIVE ENCRYPTION VS. NON-INTERACTIVE ENCRYPTION:

The dissimilarity between these two types of encryptionis that the concluding scheme does not need communicationbetween sender and receiver.

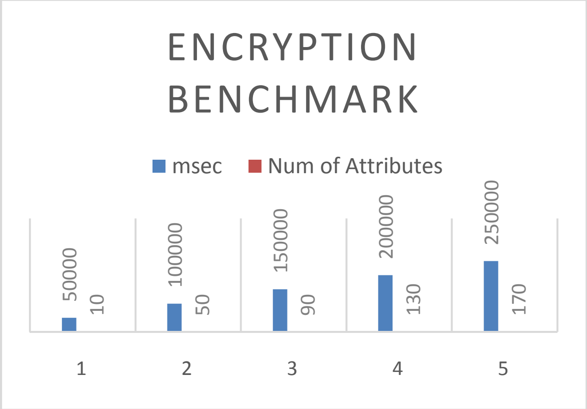
7] ALGORITHM:

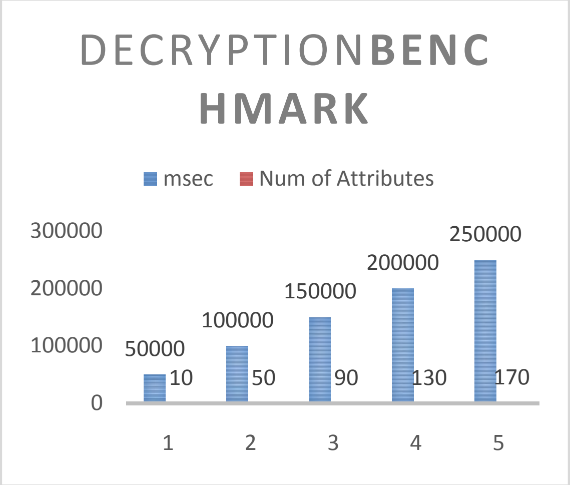
DENIABLE CP-ABE CONSTRUCTION:

To build an audit-free secure cloud storage service, we use a deniable CP-ABE scheme as our core technology. We construct our basic deniable CP-ABE scheme, which is based as follows:

Setup (1) (PP,MSK):This proceeds security parameter as info and returns open parameter as PP and framework ace key MSK.
KeyGen(MSK,S) →SK : Given arrangement of characteristics S and MSK. It produces private key SK.
Enc(PP,M,A) →C :This encryption calculation takes as info open parameter PP, message M get to structure A=(M,) over the universe of properties, This calculation encrypts M and produces a figure content C, which can be decrypted by the individuals who have a characteristic set that fulfills get to structure A. Take note of A is contained in C.
Dec(PP, SK,C) → {M,⊥}: This decryption calculation takes as information open parameter PP, private key SK with its property set S, and ciphertext C with its get to structure A. In the event that S fulfillsA, then this calculation returns M
Verify(PP,C,M, PE, PD) → {T, F}: It Is utilized to check the rightness of PE and PD
OpenEnc(PP,C,M) → PE: It is for the sender to release encryption proof PE for (M,C).
OpenDec(PP, SK,C,M) → PD: It is for the receiver to release decryption proof PD for (M,C).

8] RESULTS:





As should be obvious, encryption time and decryption time become directly over the attribute number in each of the three plans. The Composite request plan is without a doubt the most tedious plan; its execution is practically unsuitable for practical applications.

9] CONCLUSION:

The projected scheme providesa potential way to fight against depravedintrusion withthe right of privacy. We anticipate more schemes can beproduced to protect cloud user privacy. Weplanned a deniable CP-ABE scheme tomake an audit-free cloud storage service. The deniabilityfeature makes compulsionuntrue, and the ABE propertyensures secure cloud data sharing with a fine-grained accesscontrol method.

10] REFERENCES:

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” inEurocrypt, 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/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 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 Euro crypt, 2011, pp. 610–626.

P.Aparna is a student of Baba Institute Of Technology & Sciences, Visakhapatnam. Presently she is pursuing her M.Tech from this college and she received his B.Tech from Lendi Institute of Technology and Sciences, affiliated to JNT University, Kakinada in the year of (2010-2014). Her area of interest includes Cloud Computing and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. K. Satya Narayana Murthy, He has a dedicated teaching experience of three years. He completed B.Tech from GVPCOE, Vizag and M.Tech from Andhra University with distinction and act as a student organizer during M.tech Period. He had begun his Career by joining as a lecturer in BITS vizag. To his ability, he can deal with all the subjects in computer science effectively and got 85% pass percentage in educated subjects. Now he was deeply involved in doing Research, Areas of Research interests includes Data mining, Image Processing, Computer Networks & Cloud Computing. He attended several seminars and workshops and he had conducted various events and organized seminars etc.