International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 4, Issue 12, December 2016.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

# AUDIT-FREE CLOUD STORAGE VIA DENIABLE ATTRIBUTE-BASED ENCRYPTION

M.Kannan[1], D.Prasanna[2]
[1]Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.
[2]Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

**Abstract:** Cloud storage services have become increasingly familiar technology. Consequence of security, numerous distributed storage encryption strategies have been proposed to shield information and it is not accessed unauthorized clients. The strategy accepted that distributed storage suppliers are protected and can't be hacked and few authorities (i.e., coercers) may compel distributed storage suppliers to uncover client secrets or private information on the cloud. In the paper, establish to design for another storage encryption strategy and it empowers distributed storage suppliers to make convincing false client secrets to protected client protection. Coercers can't declare to get secrets are valid or not, distributed storage suppliers guarantee client protection is still safely secured. Distributed storage service suppliers or trusted third parties dealing key administration are trusted and can't be hacked. Some elements catch interchanges amongst clients and distributed storage suppliers and compel storage suppliers to release client secrets by utilizing government control. The encrypted information's are assumed to be known and storage suppliers are demanded to discharge client secrets
.

**Keywords:** Cloud storage services, key management, coercers, distributed storage suppliers, cloud, Attribute-based Encryption, Audit-Free Cloud Storage.

## Introduction:

Distributed storage services become increasingly important and clients can store their information on the cloud and any place and any time to access their information. Information stored in the cloud encoded and shielded utilizing security process and access by different clients. Attribute based encryption (ABE) viewed as the reasonable encryption strategies for distributed storage. Some elements block interchanges amongst clients and distributed storage suppliers and storage suppliers to discharge client secrets by utilizing government control. The encrypted information's are assumed to be known and storage suppliers are demanded to discharge client secrets.

When distributed storage suppliers are compromised encryption strategies lose viability. Trust distributed storage supplier's battle against substances to keep client security through legitimate avenues and it is apparently more troublesome. Lavabit was an email service organization that shielded all client messages from outside compulsion. Unfortunately, it fizzled and chose to close down its email service. It is hard to battle against outside pressure, meant to construct an encryption methodology and it helps distributed storage suppliers to avoid this kind of bind. To offer distributed storage suppliers intends making fake client secrets. The fake client secrets, outside coercers can obtain fashioned information from a client's stored ciphertext. The coercers think they got secrets are genuine and it fulfilled of all imperatively distributed storage suppliers won't have uncovered any

genuine secrets. In the manner, client security is as still ensured and an idea originates from a special kind of encryption strategy called deniable encryption. Deniable encryption containing senders and recipients making persuading fake confirmation of fashioned information in ciphertexts to an extent that outside authorities are fulfilled.

The deniability originates from the way that coercers can't demonstrate the proposed evidence isn't right and consequently have no motivation to dismiss the given confirmation. The method tries to inside and block coercion endeavors because coercers realize that their endeavors will be futile. It makes utilization of this thought with the end goal that distributed storage suppliers can give review free storage services. Distributed storage scenarios, information proprietors who store their information on the cloud are much the same as senders in the deniable encryption strategy. The persons who access to encrypted information's can assume the part of beneficiary in the deniable encryption strategy, including the distributed storage suppliers themselves, who have framework wide secrets and must have the capacity to decode all encoded data. A deniable ABE strategy portrayed for distributed storage services. To make utilization of ABE qualities for securing stored information with a fine-grained access control technique and deniable encryption to counteract outside inspecting. It depends on ciphertext strategy policy-attribute based encryption (CP-ABE). The strategy enhanced from prime request bilinear gatherings to composite request bilinear gatherings. Subgroup decision issue assumption, the proposed strategy empowers clients to have the capacity to give fake secrets that appear to be legitimate to outside coercers.

**Related Work**

Sahai et al. [1] presented the idea of ABE (Attribute Based Encryption) in which data proprietors can embed they need to share information as far as encryption. That is, the individuals coordinate the proprietor's conditions can effectively decrypt stored information. However, the ABE is encryption for privileges, not for clients. Goyal et al. [2] discussed KPABE (Key-Policy Attribute Based Encryption) and built an expressive method to relate any monotonic equation as the policy for client secret keys. However, the key is easily identified. Bethencourt et al. [3] described the principal CP-ABE (ciphertext policy-attribute based encryption) and utilized a tree access structure to express any monotonic formula over properties as the policy in the ciphertext. But, it utilized only for the attributes.

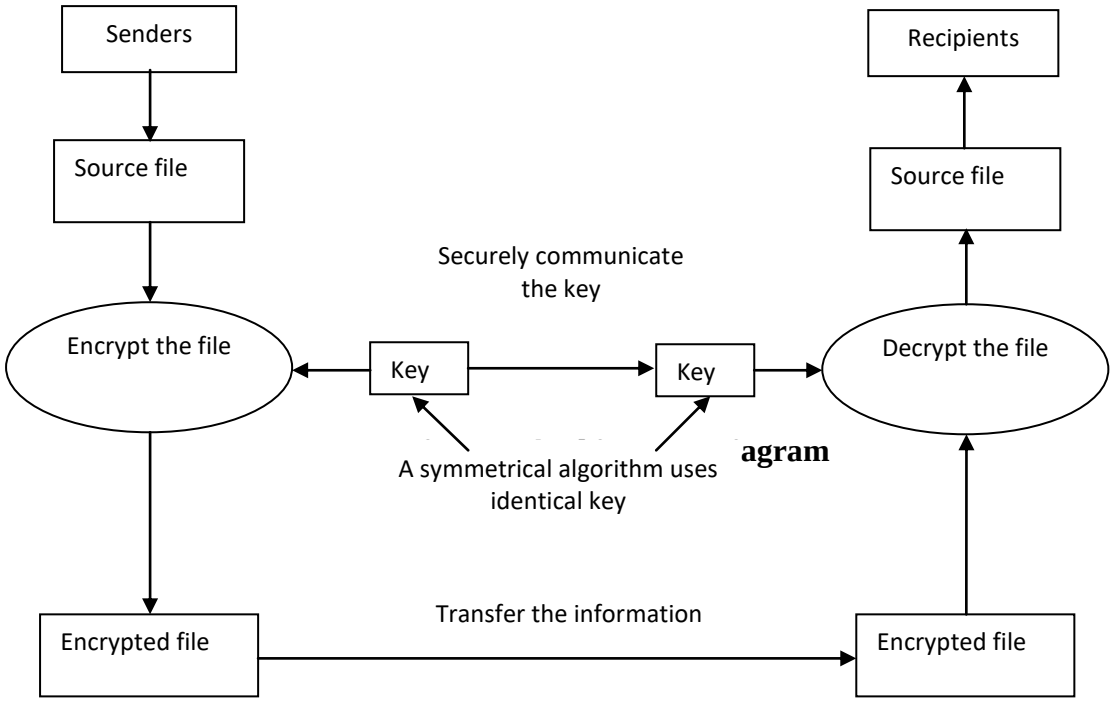
Waters [4] discussed expressive CP-ABE (ciphertext policy-attribute based encryption) and it utilized Linear Secret Sharing Schemes (LSSS) to construct a ciphertext policy. Since, it is used for ciphertext and easily breakable. Nielsen et al. [5] and Bendlin et al. [6] expressed difficult to encrypt unbounded messages by one short key in non-submitting strategies, containing deniable method. It demonstrates that non-interactive and completely recipient deniable methods can't be accomplished simultaneously.

Gasti et al. [7] introduced another deniable method in which one open private key pair is arrangement for every client while there are really two sets. The sender can transfer a genuine message encoded by one key with a fake message encrypted by the other key. Canetti et al. [8] utilized translucent sets to develop deniable encryption strategies. A translucent set is a set including a trapdoor subset. It is easy to randomly select a component from the all inclusive set or from the subset; however, without the trapdoor, it is hard to decide whether a given component has a place with the subset.

**Proposed System**

Strategies utilized as a part of deniable encryption strategies, to construct two encryption situations at the same time, much like the thought proposed in. Assemble our strategy with numerous measurements while asserting there is a single measurement. In the method eliminates obvious repetitive parts in. Apply this method to a current ABE strategy by replacing prime request groups with composite request gatherings. Because the base ABE methodology can encrypt one part every time, deniable CPABE is absolutely a blockwise deniable encryption method. The bilinear task for the

composite request group is slower than the prime request gathering, there are a few methods that can change over an encryption methodology from composite request gatherings to prime request groups for better computational performance. Figure.1 shows the architecture diagram of proposed framework.




**agram**

**Deniable Encryption**:

Deniable encryption includes senders and recipients making persuading fake confirmation of fashioned information in ciphertexts with the end goal that outside coercers are fulfilled. The deniability originates from the way that coercers can't demonstrate the proposed evidence isn't right and thusly have no motivation to dismiss the given proof. In the method tries to altogether block coercion endeavors since coercers realize that their endeavors will be futile. To make utilization of this thought with the end goal of distributed storage suppliers give review free storage services. Distributed storage situation, data proprietors store information on the cloud are much the same as senders in the deniable encryption methodology. The individuals who get to the encrypted information's can assume the component of recipient in the deniable encryption method, including the distributed storage suppliers have framework wide secrets and must have the capacity to decode all encoded information. It makes utilization of ABE behaviors for securing stored information with a fine-grained access control framework and deniable encryption to turn away exterior auditing.

**Composite order Bilinear Group**:

Requesting bilinear gatherings for constructing audit-free distributed storage services to develop a deniable ciphertext policy-attribute based encryption strategy. Dropping property utilization for building is predictable domain and attention to an important issue of computational cost for the complex request bilinear gathering. The bilinear activity of a complex demand is slower than the task of a prime request bilinear gathering. A client invests excessively energy in decoding while getting documents on the cloud. Complex request make bilinear gathering methodologies more practical, into prime request strategies. Utilizing a simulating tool proposed to change over complex demand bilinear gathering strategy to a prime request bilinear gathering methodology. The tool is depends on double orthonormal bases and the subspace supposition.

**Attribute-Based Encryption**:

Clients can store information on the cloud and access their information anyplace and anywhere. Information stored on the cloud is encrypted and shielded from access by different clients. Attribute based encryption (ABE) is viewed as the most appropriate encryption strategies for distributed storage. Some elements differentiate amongst clients and distributed storage suppliers and require storage suppliers to discharge client secrets by utilizing government control. Encrypted information's are known and storage suppliers are demanded to discharge client secrets. Trust distributed storage suppliers can battle against such elements to keep up client security through legitimate avenues and it is actually more difficult.

**Cloud Storage:**

Distributed storage services have become progressively popular. Numerous distributed storage encryption strategies have been proposed to shield information from the individuals. The strategy expected that distributed storage suppliers are sheltered and can't be hacked. Some experts (i.e., coercers) compel distributed storage suppliers to uncover client secrets or private information on the cloud. A display method for other distributed storage encryption method empowers distributed storage suppliers to make persuading fake client secrets to secure client protection. The coercers can't reveal if acquired secrets are valid or not and the distributed storage suppliers guarantee client protection is still safely ensured. Distributed storage service suppliers or trusted third parties dealing key management are trusted and can't be hacked. Plan to manufacture an encryption strategy that could help distributed storage suppliers avoid this difficulty. It offers distributed storage suppliers intend to make fake client secrets. Some fake client secrets, outside coercers can get fashioned information from a client's stored ciphertext. Coercers received privileged secrets are genuine and fulfilled. The client security is as yet ensured and an idea originates from an exceptional sort of encryption strategy called deniable encryption.

**Proprietor:**

Proprietor is to transfer documents utilizing some access policy. Initially, he/she get the general population key for specific transfer document. After, he/she gets public key proprietor demand for the secret key for specific transfer record. Utilizing, secret key proprietor transfer their document.

**Client:**

In the client is utilized to support the customer for search the document, utilizing the file id and document name. The file id and name is erroneous means don't get the document. Generally, the server request clients in general key and get the encryption record. On the chance to need the decryption record implies client have the secret key.

**Result and Discussion**

To focus on encryption and decryption performance based on data sharing and protection. The deniable CPABE works on data proprietor and client. The design does not have any reliability with cloud and its work separately for secure data sharing and retrieval in cloud infrastructure. It performs some estimation aspects such as Encryption Time and Decryption Time.

Table 1 explained the encryption time and decryption time proposed framework with closest existing methodologies. The method is investigated in terms of encryption time (in sec) and decryption time (sec) and demonstrates their average values for respective features with data types.

**Table 1 Encryption Time (ET) and Decryption Time for Text, Document and PDF data types**

| Learning Algorithm | Text | | Document | | PDF | |
|---|---|---|---|---|---|---|
| | ET | DT | ET | DT | ET | DT |
| BRUTE | 0.462 | 0.53 | 0.75 | 0.99 | 4.588 | 0.150 |
| EHI | 0.086 | 0.21 | 0.88 | 0.308 | 3.113 | 0.100 |
| CPABE | 0.08 | 0.10 | 0.575 | 0.110 | 0.19 | 0.027 |

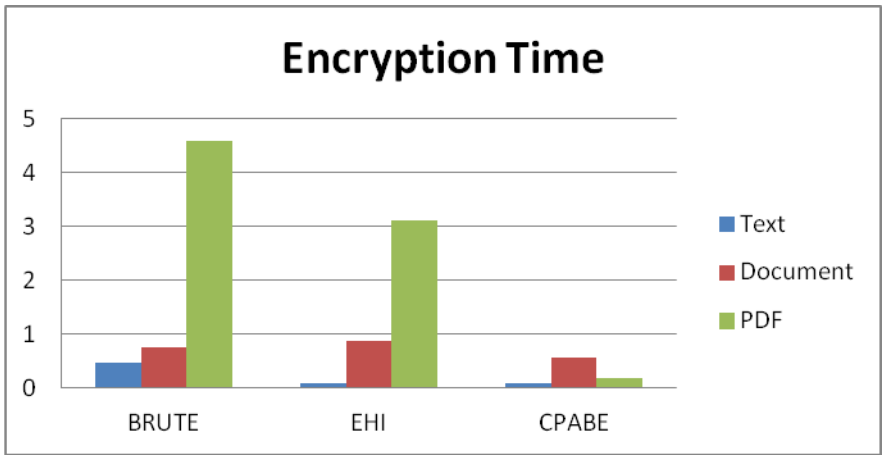



**Figure.2 Encryption time for text, document and PDF data**

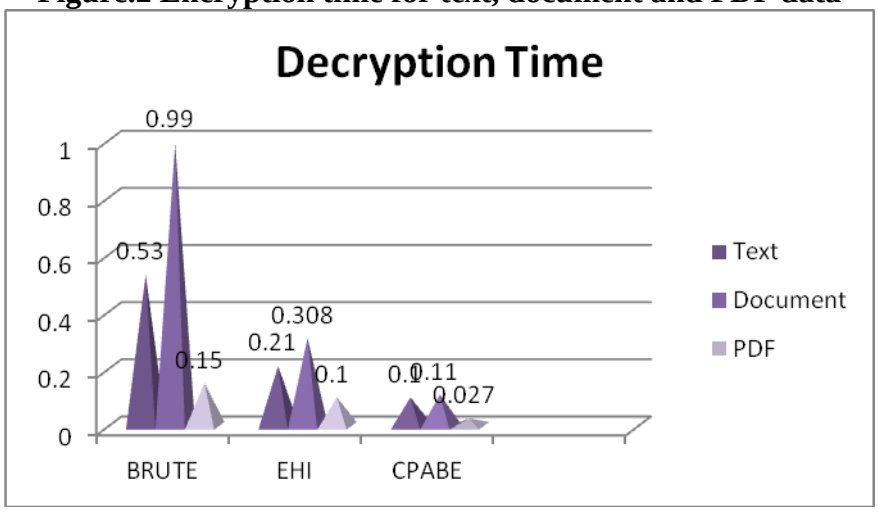



**Figure.3 Decryption time for text, document and PDF data**

Based on Table 1, Figures 2 to 3 performances, it observed that proposed CPABE is best approach for overall data kinds along with respective features. Behalf of Encryption Time (ET) and Decryption Time (DT), it noticed proposed framework closest competitor was EHI. However, result of EHI is too far comparing than our proposed CPABE. Finally, its claim that proposed CPABE is a best methodology on overall data kinds and respective aspects.

**Conclusion:**

A deniable CP-ABE method constructing an audit free distributed storage service. The deniability attributes influences coercion to invalid, and the ABE property guarantees secure cloud information sharing to a fine-grained access control technique. Proposed strategy gives a conceivable method to battle against corrupt interference with the privilege of protection. Trust more plans can be made to ensure cloud client protection.

**References**

[1]. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Eurocrypt, pp. 457–473, 2005.
[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, pp. 89–98, 2006.
[3]. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE Symposium on Security and Privacy, pp. 321–334, 2007.

[4]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, pp. 53–70, 2011.
[5]. J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in Crypto, pp. 111–126, 2002.
[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, http://eprint.iacr.org/ , 2011
[7]. P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, pp. 31– 42, 2010.
[8]. R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in Crypto, pp. 90–104, 1997.