***ABSTRACT***:

**DENIABLE ATTRIBUTE BASED ENCRYPTION WITH DATA HIDING TECHNIQUE**

**Saranya S1, Revathi A2**

**1PG student, PERI Institute Of Technology, Department of Computer science and engineering, Anna University, Chennai, India.**

**\*2*Head of the department*,Assistant Professor, PERI Institute Of Technology, Department of Computer science and engineering, Anna University, Chennai, India.**

Attribute based encryption (ABE) is a powerful encryption technique used in cloud computing, IoT, social networks and other technological fields where security and privacy are essential requirements of the system. There are different types of ABE schemes and this article highlights the features of multi-authority attribute based encryption (MA-ABE) schemes. A multi-authority ABE system consists of any number attribute authorities and any number of users. A set of global public parameters is defined in the system. A user can select an attribute authority and obtain the corresponding decryption keys. The authority executes the corresponding attribute key generation algorithm and the result is returned to the user. The encryption process uses the global public parameters and an attribute set to produce the cipher text. Decryption is performed using the decryption keys for the attribute set.

***Index Terms*-  *Deniable encryption, Attribute Based Encryption and Multi Authority-Attribute Based Encryption***

**I INTRODUCTION**

Cloud storage is a form of data storage where the digital data is stored in logical pools, the physical storage span multiple servers (and often locations), and the physical environment is typically owned and handled by a hosting organization. These cloud storage providers are answerable for keeping the data available and accessible, and the physical environment protected and running. Different organizations buy or lease storage capacity from the providers to store customer application data [1]. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API)[2] or by applications that utilize the API, such as cloud desktop storage, a gateway or Web- based content management systems. In the cloud storage environment customers can store their data on the cloud and access their data from anywhere at any time by connecting to a network [3]. Because of user privacy, the data stored on the cloud is normally encrypted and safe guarded from access by other users [4]. 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. Attribute-based encryption is a kind of public-key encryption in which the secret key of a user and the ciphertext are reliant upon attributes. In such a structure, the decryption of a ciphertext is achievable only if the set of attributes of the user key equals the attributes of the ciphertext.[5]. A central security feature of Attribute-Based Encryption is collusion-resistance: An challenger that grasps multiple keys be supposed to only be capable to access data if at least one individual key grants access. The aim choosing this attribute-based encryption is that as more responsive, data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One disadvantage of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). To overcome this disadvantage we used a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE) [6]. In this cryptosystem, cipher text are labelled with sets of attributes and private keys are associated with access structures that control which cipher text by this the user can easily able to decrypt the data which was encrypted. The applicability of this construction is to share the audit-log information and broadcast encryption and also supports delegation of private keys which includes the Hierarchical Identity-Based Encryption. These Encryption schemes assuring that cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked [7].

Attribute based encryption has been rapid developed since it was born, and it is a hot direction in cryptograph recently, which realizes non interactive fine-grained access control mechanism, expands one-to-one model to one to many model on encryption and decryption, greatly enriches the flexibility of encryption policy and description of user permissions. Hence, it has a good application prospects in distributed file management, third party data storage, pay TV system and other fields[5,6]. However, in all existing ABE schemes, all users can only get one same kind of permission if satisfying access policy. With the rapid development of network, the rise of cloud computing and different demand growth of large-scale user, it is necessary to give users different permissions.

However, in all existing ABE schemes, all users can only get one same kind of permission if satisfying access policy. With the rapid development of network, the rise of cloud computing and different demand growth of large-scale user, it is necessary to give users different permissions. For example: there are four attribute authorities monitoring four attribute sets.

**1.2 Contribution and plan of this paper**

In this paper we construct deniable scheme to overcome the problem of disclosure of the user’s original data on request by the governmental higher authorities to handover the data from cloud storage providers and we also overcome the problem of secret key being exposed to the higher authorities by using attribute based encryption. We use (MA-ABE) Multi-Authority Attribute based encryption for this. Previous deniable schemes used translucent sets while we use multidimensional space for deniable encryption. We use composite order bilinear groups to construct multidimensional space. We also use data hiding technique in order to protect the data stored in the cloud storage.

Image data hiding is a technique in which secret message is embedded inside an image. Cover Image is defined as the original image into which the required secret message is embedded. It is also termed as innocent image or host image. The secret message should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image. Good cover images range from gray scale image to colored image in uncompressed format. Stego image is the final image obtained after embedded the payload into a given cover image. It should have similar statistical properties to that of the cover image. We use Discrete Wavelet Transform (DWT) technique for hiding our data inside an image.

**II LITERATURE SURVEY**

The concept of ABE(Attribute-Based Encryption) inwhich data owners can insert how they want todistribute data in terms of encryption. That is, onlythose who match the owner’s conditions cansuccessfully decrypt stored data. We can say herethat ABE is encryption for privileges, not for users.This makes ABE a very helpful tool for cloudstorage services since data sharing is a significantfeature for such services. Cloud storage users arenot practical for data owners to encrypt their databy pair wise keys [7]. Furthermore, it is also impracticalto encrypt data many times for many people. WithABE, data owners make a decision only which kindof users can access their encrypted data. Users whoconvince the conditions are able to decrypt theencrypted data. The scheme of deniable encryptionis nothing but it also similar to common encryptionschemes, deniable encryption can be separated intoa deniable shared key scheme and a public keyscheme. Allowing the cloud storage scenario, wefocus our efforts on the deniable public keyencryption scheme. The simulatable public keysystem provides an unaware key generationfunction and an oblivious cipher text function.When transferring an encrypted bit, the sender willsend a set of encrypted data which may be usuallyencrypted or insensible. Therefore, the dispatchercan claim some sent messages are oblivious whileactually they are not. The scheme can be applied tothe receiver side such that the scheme is a bi-deniablescheme. While performing this schemethere are some disadvantages may arise. Those areComputational overhead. I.e. Encryptionparameters should be totally different for eachencryption operation. So each coercion will reduceflexibility. We can also face Decrypted data withmissing of contents at such blocks. Entities of thecloud environment may stop communicationsbetween users and cloud storage providers andthen require storage providers to release usersecrets by using power or other means. In thissituation, encrypted data are assumed to be knownand storage providers are requested to dischargeuser secrets here another disadvantage is Dataredundancy is Occur at each block of data. The noninteractive and fully receiver deniable schemescannot be achieved simultaneously. It is alsoimpossible to encrypt unbounded messages, usingone short key in non committing schemes.

The future performance scheme with Cipher Text Policy Attribute Based encryption [8] presents a cloud storage provider which means to make fake user secrets. Specified such fake user secrets, outside coercers can only obtained fake data from a user’s stored cipher text. The coercers think the received secrets are real, they will be content and more prominently cloud storage providers will not have revealed any real secrets. So, user privacy is still confined in cloud computing environment[8].

In order to overcome all these disadvantages Cipher text policy attribute-based encryption (CP-ABE) scheme is being implemented. The implementation of a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In these circumstances, cloud storage service providers will just watch as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use transparent sets or simulatable public key systems to apply deniability. Deniable Cipher Text Policy Attribute Based Encryption scheme make with two encryption environments at the same time, much like the idea planned in this scheme with many sizes while claiming there is only one size. This approach removes clear redundant parts. The base ABE scheme can encrypt one block each time; our deniable CPABE is definitely a block wise deniable encryption scheme. The bilinear operation for the Composite order group is slower than the prime order group, there are some methods that can change an encryption scheme from Composite order groups to prime order groups for improved computational performance. Deniable Cipher Text Policy Attribute Based Encryption offers a reliable environment for our deniable encryption scheme[9].

Ting Yu , Winslett, M. [10] Automated trust negotiation is an approach to establishing trust between strangers through iterative disclosure of digital credentials. In automated trust negotiation, access control policies play a key role in protecting resources from unauthorized access. Unlike in traditional trust management systems, the access control policy for a resource is usually unknown to the party requesting access to the resource, when trust negotiation starts. The negotiating parties can rely on policy disclosures to learn each other's access control requirements. However a policy itself may also contain sensitive information. Disclosing policies' contents unconditionally may leak valuable business information or jeopardize individuals' privacy.

This paper [11] proposing UniPro, a unified scheme to model protection of resources, including policies, in trust negotiation. UniPro improves on previous work by

modeling policies as first-class resources, protecting them in the same way as other resources, providing fine-grained control over policy disclosure, and clearly distinguishing between policy disclosure and policy satisfaction, which gives users more flexibility in expressing their authorization requirements. It also show that UniPro can be used with practical negotiation strategies without jeopardizing autonomy in the choice of strategy, and present criteria under which negotiations using UniPro are guaranteed to succeed in establishing trust.

In [12] several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. This paper presenting a system for realizing complex access control on encrypted data that call Ciphertext-Policy Attribute-Based Encryption. By using this techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, this methods are secure against collusion attacks.

In [13] Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, this methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, it provide an implementation of our system and give performance measurements.

In [14] introduce a new type of Identity Based Encryption (IBE) scheme that it call Fuzzy Identity Based Encryption. A Fuzzy IBE scheme allows for a private key for an identity id to decrypt a cipher text encrypted with another identity id, if and only if the identities id and id # are close to each other as measured by some metric (e.g. Hamming distance). A Fuzzy IBE scheme can be applied to enable encryption using biometric measurements as identities. The error-tolerance of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently contain some amount of noise during each measurement.

**III 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 Most of the previous deniable encryption schemes are inter-encryption independent. That is, the encryption parameters should be totally different for each encryption operation. If two deniable encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility. Most deniable encryption schemes have decryption error problems. These errors come from the designed decryption mechanisms [17].

**IV. PROPOSED SCHEME**

Most deniable public key schemes are bitwise, which means these schemes be able to process one bit a time. Hence, bitwise deniable encryption schemes are incompetent for real use, especially in the cloud storage service case. To resolve this problem, considered a hybrid encryption scheme that concurrently uses symmetric and asymmetric encryption. They use a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted by a symmetric key encryption mechanism. Mainly deniable encryption schemes have decryption error problems. These errors come from the considered decryption mechanisms. Uses the subset decision mechanism for decryption. The receiver decides the decrypted message according to the subset decision result. If the sender desires an element from the universal set but unluckily the element is located in the specific subset, then an error occurs. The identical error occurs in all transparent set- based deniable encryption schemes. Scope the policy of a file might be unused to under the request by the customer, when concluding the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The position when any of the above criteria exists the policy will be rejecting and the key director will totally withdraw from the public key of the associated file. So no one can pick up the control key of a repudiated file in future. Due to this reason we can say the file is certainly erased. To get well the file, the user must ask for the key controller to fabricate the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is confirmed by means of an attribute connected with the file.

**4.1 SYSTEM MODEL**

In this work, there is a consistent environment for

deniable encryption scheme. By consistent environment, means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look

convincing for all cipher texts under this environment, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of this scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, can construct the released fake key to decrypt normal cipher texts correctly.



Fig .1 System Architecture

**4.2 DENIABLE ENCRYPTION PROCESS**

Deniable encryption involves senders and receivers creating believable fake proof of fake data in cipher texts such that outside coercers are pleased. Note that deniability comes from the truth that coercers cannot confirm the proposed facts is incorrect and as a result no reason to decline the given evidence. This approach tries to overall block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can give audit-free storage services. In the cloud storage situation, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing.

**4.3 COMPOSITE ORDER BILINEAR GROUP**

Design a deniable CP-ABE scheme with Composite order bilinear groups for building audit-free cloud storage services. Composite order bilinear groups contain two attractive properties, namely projecting and cancelling. We make use of the cancelling property for building a consistent environment; on the other hand, Freeman also pointed out the important problem of computational cost in regard to the Composite order bilinear group. The bilinear map operation of a Composite order bilinear group is much slower than the operation of a prime order bilinear group with the same security level. That is, in this scheme, a user will pay out too much time in decryption when accessing files from the cloud. To make Composite order bilinear group schemes more realistic, into prime order schemes. Both projecting and cancelling cannot be simultaneously achieved in prime order groups in. For the same reason, we use a simulating tool projected to convert our Composite order bilinear group scheme to a prime order bilinear group scheme. This tool is based on dual orthonormal bases and the subspace assumption. Unlike subgroups are simulated as different orthonormal bases and therefore, by the orthogonal property, the bilinear operation will be cancelled between different subgroups. Our formal deniable CP-ABE construction method uses only the cancelling property of the Composite order group.

**4.4 ATTRIBUTE-BASED ENCRYPTION**

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. For the reason of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the mutual property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are several ABE schemes that have been proposed, including. Most of the proposed schemes assume cloud storage service providers or trusted third parties managing key management are trusted and cannot be hacked; yet, in practice, some entities may cut off 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 understood to be known and storage providers are requested to release user secrets[6].

**4.5 CLOUD STORAGE**

Cloud storage services have grown popularly. For the reason of the importance of privacy, many cloud storage encryption schemes have been projected to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked. Still, in practice, some authorities (i.e., coercers) may force cloud storage providers to expose user secrets or confidential data on the cloud, thus in total circumventing storage encryption schemes. Here we present a design for a new cloud storage encryption scheme that enables cloud storage providers to generate realistic fake user secrets to protect user privacy. As coercers cannot tell if obtained secrets are correct or not, the cloud storage providers make sure that user privacy is still firmly protected. Most of the projected schemes guess cloud storage service providers or trusted third parties managing key management are trusted and cannot be hacked;.

**4.6 DISTRIBUTED MULTIPLE ATTRIBUTE POLICY ATTRIBUTE BASED ENCRYPTION**

MA-ABE is a public key cryptography primitive for one-to-many correspondences. In MA-ABE, information is associated with attributes for each of which a public key part is described. The encryptor acquaintances the set of attributes to the message by scrambling it with the comparing public key parts. Each client is assigned an access arrangement which is normally characterized as an access tree over information attributes. Client secret key is characterized to reproduce the access structure so the client has the skill to decipher a cipher-text if and just if the information attributes fulfill his access structure.

**4.7 ALGORITHMS**

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

Setup (1) -> (PP,MSK):This algorithm takes security parameter as input and returns public parameter as PP and system master key MSK. Key Gen(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 LSSSaccess 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 A is contained in C. Verify(PP,C,M, PE, PD) → {T, F}:

This algorithm is used to verify the correctness of PE and PD Open Enc(PP,C,M) → PE:

This algorithm is for the sender to release encryption proof PE for (M,C).Open Dec(PP, SK,C,M) → PD:

This algorithm is for the receiver to release decryption proof PD for (M,C). 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.

**4.8 ACHIEVEMENTS BY MULTIPLE ATTRIBUTE POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME**

We can achieve high Computational performance. While using this scheme no security violence will occur. Deniable Multiple Attribute Policy Attribute Based Encryption construct at reliable environment. Reliable environment which means that one encryption environment can be worn for multiple encryption times exclusive of system updates. No error occurrences will face in decryption level. There is no data redundancy. The opened receiver verification should look believable for all cipher texts under this situation, apart from of whether a cipher text is usually encrypted or deniably encrypted. The deniability of this scheme comes from the secret of the subgroup task, which is resolute only once in the scheme setup phase. With this cancelling property and the proper subgroup assignment, we can construct the released false key to decrypt normal cipher texts correctly Deniable Cipher Text Policy Attribute Based Encryption Extends a pairing ABE, which has a deterministic decryption algorithm, from the prime order group to the Composite order group. The decryption algorithm in this scheme is still deterministic; hence, there is no decryption errors using this scheme.

**V. IMPLEMENTATION**

The proposed system of this project is divided into Five major modules and described as below.

1. **DATA OWNER**
2. **CLOUD SERVER**
3. **DATA INTEGRITY**
4. **MA-ABE**
5. **DATA CONSUMER**

**5.1 MODULES DESCRIPTION**

**5.1.1 DATA OWNER**

In this module, the cloud server adds data owner by Registering with their details like owner name, password, email, organization and address, The Data owner Logins by user name and password. The data owner browses and uploads their data in the cloud server by providing details Domain (Cloud computing, Data mining, networking, sensor networking, adhoc networking), Technology (Java, Dot net, SAP, PHP, NS2), Author name and publication. For the security purpose the Data owner encrypts data as well as encrypted keyword-index stores to the cloud Server.

**5.1.2 CLOUD SERVER**

The cloud server is responsible for data storage andfiles authorization and file search for an end user. Theencrypted data file contents will be stored with theirtags such as file name, domain, Technology, Author,Publication, secret key, digital sign, date and time andowner name. The data owner is also responsible foradding data owner and to view the data owner files.The owner can conduct keyword search operations onbehalf of the data users, the keyword search based onkeywords (Author, Technology, Domain, publishers)will be sent to the Trust authority. If all are true then itwill send to the corresponding user or he will becaptured as attacker. The cloud server can also act asattacker to modify the data which will be auditing bythe audit cloud.

**5.1.3 DATA INTEGRITY**

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

**5.1.4 MA-ABE**

The MA-ABE allows clients and cloud applications to simultaneously data user services from and route data

to cloud. Module issues credentials to the data users. The credentials are sent over authenticated private channels. It is responsible of searching, requesting the file to cloud server, generating secret key for each and every files based on data owner and provides to the Data user.

**5.1.5 DATA CONSUMER (DATA USER/END USER)**

In this module, the user is responsible of searching the files in cloud server by providing attributes like Technology, author name, publisher, Domain(cloud computing, network security,). The data consumer can request the secret key to cloud server via MA-ABE and then the Data Consumer can access the data file with the encrypted key, so if User access the file by wrong Key then the user will consider as malicious users and blocked the User.



Fig. 2 Welcome Page



Fig.3 Register Page

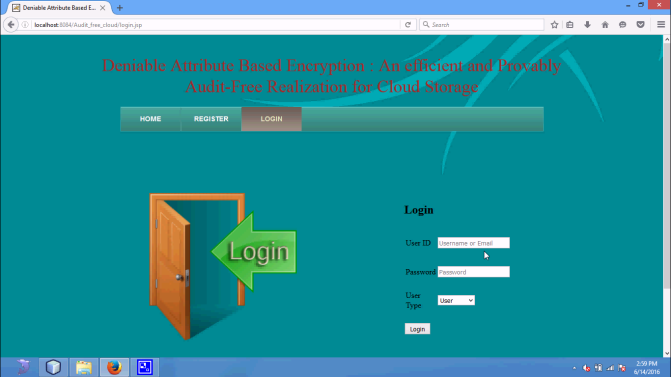


Fig.4 Login page

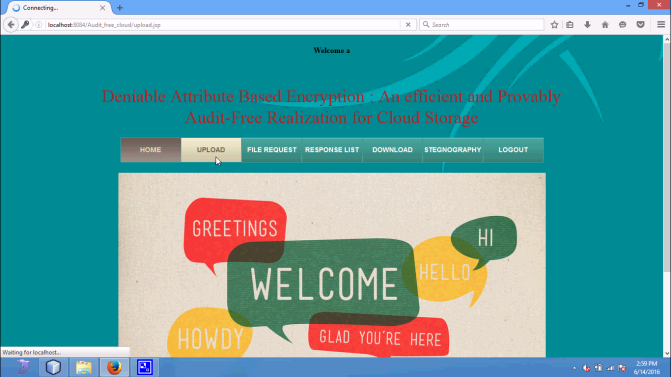


Fig.5 Data Owner

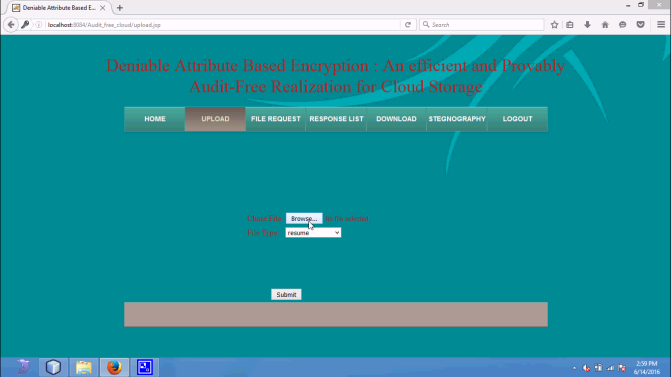


Fig .56 Upload

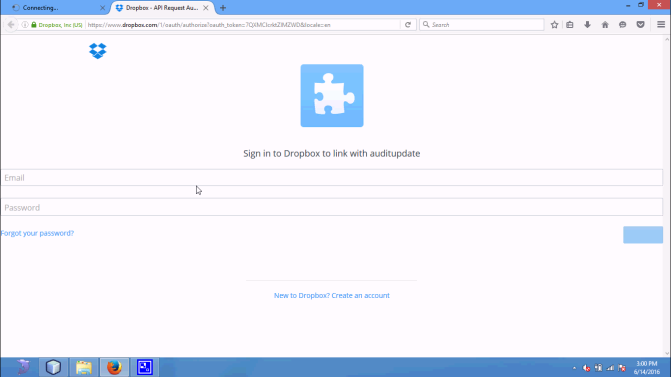


Fig.7 cloud login



Fig. 8 Request file

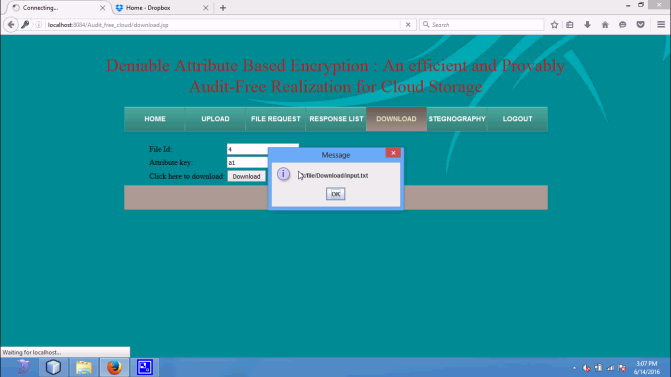


Fig. 9 download



Fig 10 Stenography – Merging Hide image

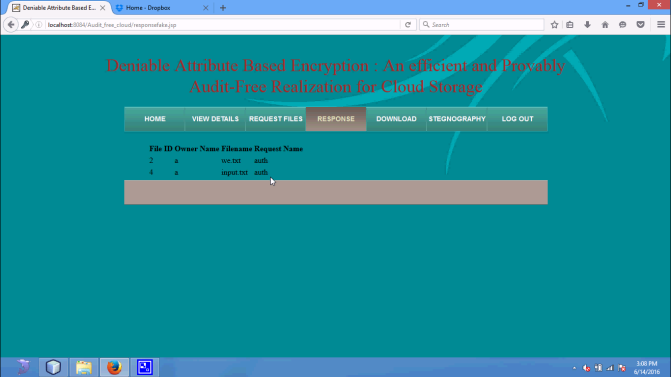


Fig .11 Auth review



Fih.12 Provider acceptance



Fig .13 Authentication response

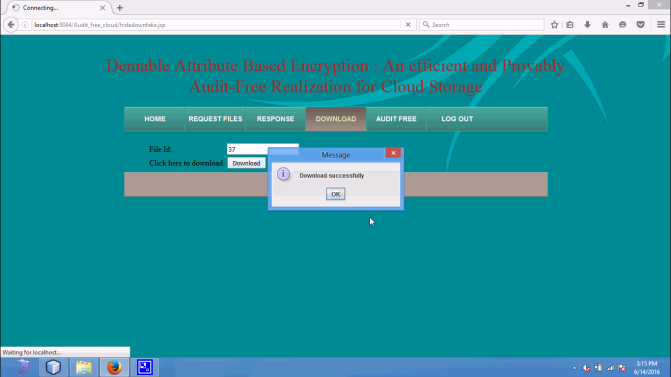


Fig.14 Results

**VI CONCLUSION**

A deniable MA-ABE scheme is an audit-free cloud storage service. The deniability feature makes force invalid, and the Attribute Based Encryption belongings guarantee secure cloud data sharing with a fine-grained access control method. This scheme presents a likely way to struggle next to dissipated intervention with the right of privacy. Not only the above can this scheme be formed to guard cloud user privacy with high computational performance.

**VII REFERENCE**

[1] V. Goyal, O. Pandey, A. Sahai, B.Waters, “Attribute-based encryption for fine-grained access control of encrypted data”. In: *ACMCCS 2006*, pp. 89-98 (2006).

[2] M. Abdalla, E. Kiltz, and G. Neven , “Generalized key delegation for hierarchical identity based encryption”. In *Computer Security* ESORICS, pages 139-154, 2007.

[3] S. Al-Riyami, J. Malone-Lee, and N. Smart. “Escrow-free encryption supporting cryptographic workflow”. In *Int. J. Inf. Sec*., volume 5, pages217-229, 2006.

[4] W. Bagga, R. Molva, and S. Crosta. “Policy-based encryption schemes from bilinear pairings”. In *ASIACCS*, page 368, 2006.

[5] J. Bethencourt, A. Sahai, and B. Waters. “Ciphertext-policy attributebased encryption In *IEEE Symposium on Security and Privacy*, pages321-334, 2007.

[6] D. Boneh and X. Boyen. “Efficient selective-id secure identity based encryption without random oracles”. In *EUROCRYPT*, pages 223- 238, 2004.

[7] D. Boneh and X. Boyen. “Secure identity based encryption without random oracles”. In*CRYPTO*, pages 443-459, 2004.

[8] D. Boneh, X. Boyen, and E. Goh. “Hierarchical identity based random oracles”. In*CRYPTO*, pages 443-459, 2004.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. “Public key encryption with keyword search”. In *EUROCRYPT*, pages 506- 522, 2004.

[10] D. Boneh and M. Franklin. “Identity based encryption from the weil pairing”. In *CRYPTO*,pages 213-229, 2001.

[11] D. Boneh, A. Sahai, and B. Waters. “Fully collusion resistant traitor tracing with shortciphertexts and private keys”. In *EUROCRYPT*, pages 573-592, 2006.

[12] R. Bradshaw, J. Holt, and K. Seamons. “Concealing complex policies with hidden Credentials”. In *ACM Conference on* *Computer and Communications Security*, pages146-157,2004.

[13] J. Camenisch and A. Lysyanskaya. “An efficient system for nontransferable anonymous credentials with optional anonymity revocation”, In: *EUROCRYPT*, 2001

[14] M. Chase. “Multi-authority attribute based encryption”. In *TCC*, pages 515-534, 2007.

[15] M. Chase and S. Chow. “Improving privacy and security in multiauthority attribute- based encryption”. In *ACM Conference on* *Computer and Communications Security*, pages 121-130, 2009.

[16] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. “Building efficient fully collusion resilient traitor tracing and revocation schemes”. In *ACM Conference on Computer* *and Communications Security*, pages 121-130, 2010.

[17] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded cipher text policy attribute-based encryption. In *ICALP*, pages 579-591, 2008.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters. “Attribute Based Encryption for Fine Grained Access Conrol of Encrypted Data”. In *ACMconference on Computer and Communications Security*, pages 89-98, 2006.

[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption”. In *EUROCRYPT*, pages 62-91, 2010.