International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Verifiable Mechanism for Attribute Based Encryption in Cloud Computing

[1] S.Boominathan [2] Dr. S.Aranganathan
[1] Department of Network Security [2] Department of Computer Science and Engineering
[1][2] B.S Abdur Rahman University, Vandalur -48
[1] boominath10@gmail.com,[2] aranga@bsauniv.ac.in

Abstract: **Cloud computing technology brings innovative computing facilities to the management of the data resources. In the computing environments, the cloud servers can offer various data services such as remote data storage, outsourced delegation, computing applications. sharing and retrieving the data are ensure with Ciphertext Policy- Attribute Based Encryption (CP-ABE), Verifiable Delegation (VD) which helps in data isolation and the verifiability of entrustment on fraudulent cloud servers. In the cloud, for achieve access control and trust data top secret, the data owners could take up attribute-based encryption to encrypt the stored data. During the encryption process the access policies may not be flexible enough. The proposed secure outsourced ABE technique addresses on key issuing and Attribute-based encryption (ABE) with outsourced decryption not only enables fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of ciphertext size and decryption cost) of the standard ABE schemes. In particular, an ABE scheme with outsourced decryption allows a third party (e.g., a cloud server) to transform an ABE ciphertext into a (short) ElGamal-type ciphertext using a public transformation key provided by a user so that the latter can be decrypted much more efficiently than the former by the user.**

Keywords: **Attribute based encryption, proxy re encryption, lazy re-encryption, key policy attribute based encryption, cipher text policy attribute based encryption, Hierarchical attribute based encryption.**

I. INTRODUCTION

Cloud computing means "a type of Internet based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet. Cloud security is the security principles applied to protect data, applications and infrastructure associated with cloud computing environments.

The data servers can be trusted to keep data confidential and enforce access control policies correctly. However, this assumption is no longer true today since services are increasingly storing data across many servers that are shared with other data owners. An example of this is cloud data storage where cloud service providers are not in the same trusted domains as end users, and hardware platforms are not under the direct control of data owners. To mitigate users privacy concerns about their data, a common solution is to store data in encrypted form so that it will remain private, even if data servers or storage devices are not trusted or compromised.

The encrypted data, however, must be amenable to sharing and access control. In identity based encryption public key is obtained from publicly known identity, private key is obtained from public key [2]. The example of identity based encryption is email address which is public key and password is private key. In key policy attribute based technique policies are associated with keys and attribute are associated with cipher text [3]. Cipher text attribute based encryption policies are associated with cipher text and attribute are associated with keys [4]. Hierarchical attribute based encryption is combination of hierarchical identity based encryption and cipher text policy attribute based encryption [5]. When data owner stores data in cloud server, user asks external audit party to maintain integrity of data. Without reading data content third party auditor should generate the audit report.

A new way for public-key encryption is used as key-aggregate cryptosystem (KAC) [1]. The encryption is done through an identifier of Ciphertext known as class, with public key. The classes are formed by classifying the ciphertext. The key owner has the master secret key which is helpful for extracting secret key. So in above scenario now the alice can send a aggregate key to bob through a email and the encrypted data is downloaded from dropbox through the aggregate key is shown in fig 1.

The user must provide the access rights to the other user as the data is encrypted and the decryption

key should be sent securely. For an example Alice keeps private data i.e. photos on dropbox and she doesn't want to share it with everyone. As the attacker may access the data so it is not possible to rely on predefine privacy preserving mechanism so all the photos were encrypted by encryption key while uploading it.

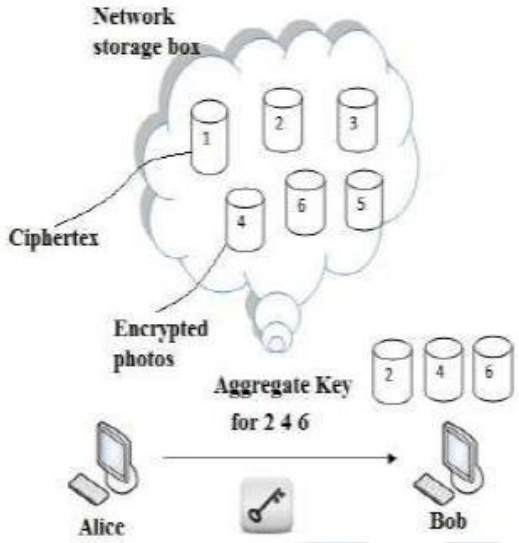


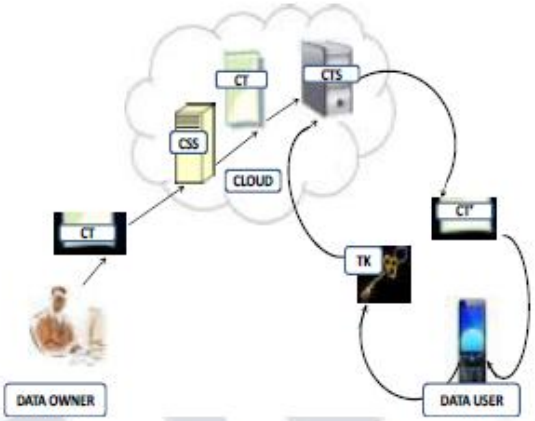
Fig .1.File sharing between Alice and Bob

II. ARCHITECTURE OF VERIFIABLE ATTRIBUTE BASED ENCRYPTION

There are two verifiable attribute based encryption schemes are available one is the trust of the attribute in web site and the second is based on trust attribute from the access policy to cipher text. Data owner find the trust attributes in websites using Trust attribute Detection Techniques then encrypts the file based on trust attributes uploads the file in cloud [3]. User decrypts the file from the cloud using trust attributes based decryption.

A users private key is split into a "transformation key" (denoted by TK), and an ElGamal-type secret key (denoted by DK). The transformation key can be publicly shared with a proxy, called Ciphertext Transformation Server (CTS), while the secret key DK must be kept private by the user. ABE ciphertexts are stored in a Cloud Storage Server (CSS). A ciphertext CT stored in the CSS is first submitted to the CTS which uses the key TK to transform CT into a simple and short El Gamal-type ciphertext CT of the same message, instead of being decrypted by the user directly. From CT , the user is able to recover the message using the secret key DK with just one exponentiation operation.

The user's transformation key can transform any ABE ciphertext satisfied by user's attributes, without revealing any information of the underlying message to malicious CTS. Thus, the user saves both bandwidth and local computation time significantly. The term ABE with outsourced decryption and the term outsourced ABE interchangeable.



Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share to a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users.

The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

A. Modules

- Registration
- Upload files
- ABE for Fine-grained Data Access Control
- Setup and Key Distribution

B. Modules Description Registration

There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf node is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to the dropbox.

Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.PUD - public domains, PSD personal domains, AA - attribute authority, MA-ABE - *multi*-authority ABE, KP-ABE key policy ABE.

C. Upload files

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted files to the server. Each owner's file encrypted both under a certain fine grained model.

Fig.3:Setup and Key Distribution

There are two ways for distributing secret keys. First using the cloud service, a Data owner can specify the access privilege of a data reader in PSD, and let application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs key gen of KP-ABE to generate the user secret key that embeds access structure.

D. Implementation Of Trust Based Attribute Based Encryption

To implement trust attribute based encryption consider hospital web site as example observations in "home page", "contact us" and "privacy policy" pages trust attributes are present [6]. In a different format and different purpose the trust attributes are present in web site Built trust attribute of website based on ability, integrity and benevolence. Belief in skills of trusted party is known as ability. Belief in rules of conduct (honesty and keeping promises) of trusted party is known as integrity. Belief in making profit and wants to do good for the customer is known as benevolences. Consider a company website as example from that website finding trust attribute. Trust attributes are classified into three types Information based (IB), Function based (FB) and not classified (NC).Images and Text and images in website is classified as information based attribute. Data encryption and web site navigation is classified as Function based. Accuracy, competency, and competency

Step-1: In application server user can access the file after authentication.

Step-2: From user database, authorized user category and user attributes.

Step-3: Value of integrity of cloud service is obtained by verifying browser service which is provided by cloud.

Step-4: Based on user activates on cloud trust of user is verified and trust values of user are calculated based on threshold and user policies.

Step-5: Based on historical data access of file trust of user is analysed. The user can access the file based on access control policies and categorization.

Step-6: Data owner encrypts the file based on trust attribute based encryption. In this encryption is done by passing trust attribute as key. The key size is based on number of trust attributes used.

III. PERFORMANCE ANALYSIS OF ATTRIBUTE BASED ENCRYPTION

Formally describe our verifiable outsourced ABE system ABEVO=(Setup, Encrypt, KeyGen, Transform, Decrypt) in Fig.2. and its security proof. Correctness: The correctness of the above ABE system follows directly from the correctness of the underlying outsourced ABE system ABEO and the correctness of the underlying symmetric encryption scheme SE. Efficiency: Compared with the underlying ABE system, the new ABE only introduces one hash value (i.e., the verification key) to the ciphertext and two hash value computations in the final decryption operation at the user side. Security Analysis Theorem 1: Suppose that the underlying outsourced ABE system is (selectively) CPA-secure, H is a family of pair wise independent hash functions, SE is a semantically secure one-time symmetric encryption scheme.

TABLE.1.COMPARISON OF ABE SCHEME

Techniques/ parameter	ABE	KP-ABE	CP-ABE	HABE	MA-ABE
Fine grained access control	Low	Low, high if there is re-encryption technique	Average realization of complex access control	good access control	Better access control
Efficiency	Average	Average, high for broadcast type system	Average, not efficient for modern enterprise environments	Flexible	Scalable
Computational overhead	High	More of computational overheads	Average computational overheads	Some of overheads	Average
Collusion resistant	Average	Good	Good	good	High collusion resistant

The performance of trust based attribute based encryption is based number of attribute and time taken to encrypt and decrypt the file. The execution time of trust based attribute encryption is less compare cipher

text attributes based encryption and key policy attributes based encryption [4]. Security of Trust attribute based encryption is high compare to cipher text attributes based encryption and key policy.

The outsourced CP-ABE scheme proposed by Green. Applying our generic construction, we immediately derive a new CP-ABE scheme supporting both outsourced decryption and verifiability as given in Fig.2.In our instantiation, the underlying ABE encrypts one group element, which may not have sufficient (computational) entropy for extracting a symmetric key. Nevertheless, we can simply extend it to a random key with enough entropy via an efficient pseudorandom number generator (e.g., AES). proposed a simple and generic method to convert any ABE scheme with non- verifiable outsourced decryption to an ABE scheme with verifiable outsourced decryption in the standard model. To concretely assess experiment results showed that our method is nearly optimal in the sense that it introduces minimal overhead in exchange for verifiability

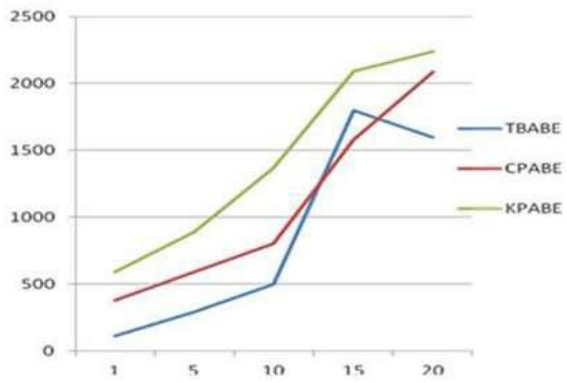
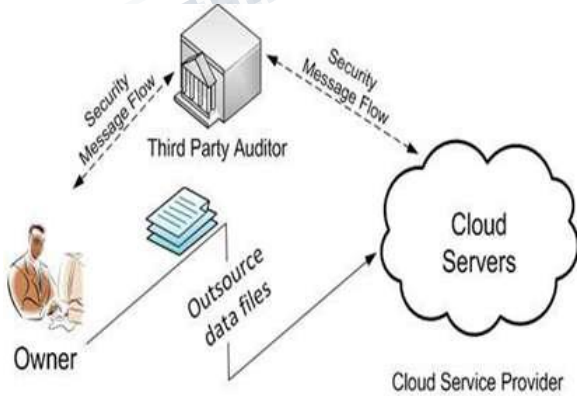


Fig.4: Number of attributes Vs execution in ms

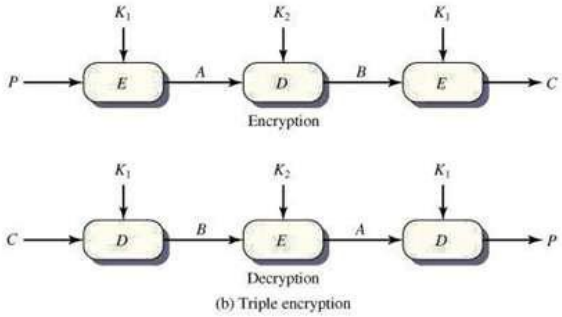
A. Verifiability

Data owner has to audit data integrity of the received data from the server.



(a) Cloud Storage Verification

Attributes based encryption because encryption is based on trust attributes [5]. create and define new access policy based on behavior of user and history of the user. Fine gained access control is achieved depending on access policy [9]. User access privileges and confidentiality is achieved by trust attribute based encryption. User secret key accountably achieved by trust attribute based encryption protect the key user.



(b) Triple encryption

IV. TRIPLE DATA ENCRYPTION ALGORITHM

Triple Data Encryption Algorithm is also known as Triple DES. Here Data Encryption Standard (DES) cipher algorithm is repeatedly applied three times to each data block. The key size of DES was generally 56 bits but Triple DES provides a relatively simple method of increasing the key size to protect against the attacks such as Brute Force attacks.

In general Triple DES algorithm uses three different keys

(3 keys{k1, k2, k3}) that has the key length of 168 bits that is of the three 56 key bits in DES. The encryption algorithm is: Cipher-text = EK3(DK2(EK1(plaintext)The plaintext is first encrypted using K1, this produces the cipher-text which in turn is decrypted with K2 and the outcome is then again encrypted with K3, the result of which is termed to be as cipher-text. The decryption algorithm is: The decryption algorithm is the reverse procedure of the encryption algorithm by using 3 keys.Plaintext = DK1(EK2(DK3(cipher-text))) Here the cipher-text that is produced by the encryption algorithm is decrypted by using K3, by using K2 the outcome of which is encrypted and the result is again decrypted with the help of the key K1, which finally produces the plaintext. Each Triple Encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last which improves the strength of algorithm when used key options 2 and provides backward compatibility with DES with key option 3. There are 3 sets of key options.

1. All three key are independent.

2. K1 and K2 are independent and K3=K1.
3. All three keys are identical K1=K2=K3.

In the case of 1 All three keys are independent is the strongest key option with 3x56=168 independent key bits. The option 2 provides less security 2x56=112 key bits, it also protect against meet in middle attacks.

This method satisfies the following requirements. Confidentiality: As the complexity of the pairing operation increases, it will be very difficult for the malicious third party to read or hack the encrypted content even thought eavesdrop on communication between the client and the sever. Authentication: As the document owner's attributes is used as the private key to encrypt the data which also server's as partial digital signature, as and when the data is decrypted by the data owner, he will be satisfied with the content as he has used his own attribute to encrypt it. Verifiability: Check sum is widely used to verify whether the content that is encrypted and the content that is been received by the data owner is same. Performance Evaluation: In order to evaluate the performance of CP-ABE scheme with verifiable outsourced decryption.

V. RESULT AND ANALYSIS

In this paper, first formalize a security model of ABE with verifiable out-sourced decryption by introducing a verification key in the output of the encryption algorithm. The present approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general, and almost optimal. traditional DES and AES algorithms are smaller in key sizes results in lesser security. It helps to ensure the data owner's data being stored in the cloud is valid or not. Data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research are yet to be identified in future.

VI. CONCLUSION

Cloud computing is the fastest growing technology in current scenario. Popular companies providing the cloud service to the users using low level encryption algorithm techniques, This leads to problematic for user storage data stored in the cloud. The proposed algorithm defines the newest level to protect the security for the cloud storage users with the multi level authentication's and the key authorization to decrypt the data in secure process. Experiment results showed that our method is nearly optimal in the sense that it introduces minimal overhead in exchange for verifiability.

REFERENCES

[1] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 8, August 2013.

[2] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proceedings of IEEE Security and Privacy, (2007), Oakland.

[3] G. Wang, Q. Liu and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", Proceedings of the 17th ACM conference on Computer and communications security, (2010), Chicago, USA.

[4] R. Bobba, H. Khurana and M. Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", Proceedings of the 14th European conference on Research in computer security, (2009), Heidelberg.

[5] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, Vol. 30, Issue 5, (2011) July, pp. 320–331.

[6] S. Muller, S. Katzenbeisser and C. Eckert, "Distributed Attribute-Based Encryption", in International Conference on Information Security and Cryptology, (2008) December 3-5, Seoul, Korea.

[7] S. Yu, C. Wang, K. Ren and W. Lou, "Attribute Based Data Sharing with Attribute Revocation", 5th ACM Symposium on Information, Computer and Communications Security, (2010) April 13 – 16, Beijing, China.

[8] G. Wang, Q. Liu and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", Proceedings of the 17th ACM conference on Computer and communications security, (2010) October 4-8, New York, USA.

[9] P. Rohini, "Data Security Technique in cloud storage", IJCST, Vol. 4, (2013), pp. 1