International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 41 (AVALON) (March 2016), PP. 57-61

ATTRIBUTE-BASED ENCRYPTION WITH VERIFIABLE OUTSOURCED DECRYPTION

Abha Pandit[1], Aishwarya Lamture[2], Pooja Sankpal[3], Shubham Dixit[4], Tabassum Maktum[5]
[1,2,3,4,5]Department Of Computer Engineering, Terna Engineering College, University Of Mumbai
Nerul, Navi Mumbai, India.
ahpandit4@gmail.com
aishwarya9m@gmail.com
poojassankpal@gmail.com
shubhamdixit1812@gmail.com
tabsmaktum@gmail.com

Abstract— **ABE is a relatively recent approach that reconsiders the concept of public-key cryptography. It basically provides access to a document if and only if the user attributes (e.g. Email ID, DOB or the country he lives in) satisfies the access policy defined by the owner of the document. Access policy is the combination of attributes (generally defined using AND/OR logical operations) using which the document can be decrypted. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently proposed ABE system with outsourced decryption largely eliminates the decryption overhead of server. In such system, the proxy server such as cloud service provider is present which has a transformation key. Any cipher text encrypted using ABE with outsourced decryption scheme into a simple cipher text. This intermediate cipher text can be transformed into plaintext by proxy server. This process incurs a small computational overhead. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious proxy) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. We also consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption.**

Index terms- **Attribute-based encryption, outsourced decryption, verifiability.**

I. INTRODUCTION

Attribute Based Access Control (ABAC) is a scheme that provides logical access control. It is distinguishable because it controls access to objects by checking the rules against the attributes of object, operations, and the environment related to a request. ABAC systems are capable of imposing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) methods. ABAC enables precise access control, which allows for a higher number of discrete inputs into an access control structure, providing a bigger set of possible combinations of those variables to reflect a larger and more definitive set of possible rules to define policies. The access control policies that can be implemented in ABAC are restricted only by the computational language and the bounty of the available attributes. This docility enables the enormous number of subjects to access the sheer number of objects without specifying individual relationships between every subject and every object. For example, a subject is assigned a set of subject attributes upon employment (e.g., Sarah is a tester in the ITIS Department). An object is assigned its object attributes upon creation (e.g., a folder with finance Records of ABE project). Objects may receive their attributes either directly from the creator or as a result of automated scanning tools. The uploader or owner of an object determines an access control policy using attributes of subjects and objects to render the set of allowable capabilities (e.g., all trainees in the ITIS Department can View the finance Records of ABE project). Under ABAC, access decisions can change between requests by just changing attribute values, without the need to modify the subject/object relationships defining underlying rule sets. This gives a more dynamic access control management capability and restricts long-term maintenance requirements of object security. Further, ABAC enables object owners/administrators to assign access control policy without prior knowledge of the particular subject and for an unlimited number of subjects that might need access. As new subjects join the system, rules and objects do not need to be changed. As long as the subject is assigned, the attributes require access necessary objects (e.g., all trainees in ITIS Department are assigned those attributes), no changes to existing rules/object attributes are required. This advantage is often referred to as accommodating the external (unanticipated) user and is one of the primary advantages of employing ABAC. [1]

ABE is a new public key following one to many (1-N) encryptions that enables access control over ciphertexts using access policies and ascribed electronic versions of their papers. There are two kinds of ABE Schemes namely, key-policy ABE (KP-ABE) [2] and ciphertext-policy ABE (CP-ABE). In a CP-

ABE scheme, each cipher-text is related with an access policy on attributes, and each user's private key is related with a set of attributes. A user is able to decrypt ciphertext only if the set of attributes related with the user's private key passes the access control policy related with the ciphertext. Whereas In a KP-ABE, the roles of an attribute set and an access policy are swapped from what we mentioned for CP-ABE: set of attributes are used to annotate the ciphertexts and access polices over these attributes are related with users' private keys. In the following, we will use the terms access control policy, access structure and access formula conversely.

One of the main failing of the most existing ABE schemes is that decryption is costly for resource-limited devices because of pairing operations and the number of pairing operations required to decrypt a ciphertext increases with the complexity of structure of access policy. At the cost of security, only proven in a weak model, there prevail several expressive ABE schemes [3] where the decryption algorithm only needs a constant number of pairing calculations. Recently, Green et al. [8] introduced a solution to this problem by introducing the idea of ABE with outsourced decryption, which chiefly removes the decryption overhead for users. Based on the former ABE schemes, Green et al. also presented solid ABE schemes with outsourced decryption. In these (refer to Fig. 1.a below), a user provides an untrusted server, a proxy operated by a cloud, with a transformation key TK that allows the latter on to translate any ABE ciphertext CT satisfied by access policy/use attributes or into a partially decrypted ciphertext/simple ciphertext CT', and it only creates a small overpower for the user to re-obtain theplaintext from the transformed ciphertext CT'.The protection property of the ABE scheme with outsourced decryption assures that an attacker (including the malicious cloud server) won't be not able to know anything about the encrypted message; but the scheme doesn't provide assurance on the correctness of the transformation performed by the cloud server. In the cloud computing setting, service providers may have strong motivation to return incorrect answers, if such answers don't require much work and are not likely to be detected by users.

Consider a web based system in which employee's details are protected using ABE schemes with outsourced decryption (e.g., [7]) and are stored in the cloud. In order to efficiently access employee's data, a user has to provide set of attributes and those must satisfy the access policy defined for the data user wants to access. For example, user attributes can be email-id, phone no, DOB and employee's designation and access policy can be ((email-id ^ (designation=programmer)) ^ (phone no ∨ DOB)). If the attribute provided by the user passes this access policy then only he can access related data. But this system does not give guarantee of correct verification. We assert an ABE with secure outsourced decryption does not always give guarantee of verifiability (i.e., correctness of the transformation performed by the cloud server). For example, the secure ABE schemes with outsourced decryption proposed by Green et al. in [8] are not verified.

II. AIMS AND OBJECTIVES

In this project, we address security factor which is basically important factor of cloud computing. Security of particular data basically means protecting data, e.g. database, from the unwanted actions of unauthorized users. Basically there are three security goals i.e. Confidentiality, Integrity, Authentication. Our objective is to implement authentication algorithm in our project. Attribute Based Encryption is an efficient security algorithm but it creates overhead on the user of the system. Hence, to overcome this drawback; ABE with outsourced decryption was introduced. But outsourcing does not guarantee correctness of the decrypted cipher text. Hence, the notion of ABE with Verifiable Outsourced Decryption was proposed. We address this scheme in our project.

III. LITERATURE REVIEW

3.1 Access Control Policies-

Access control models can be traditionally categorized into three types:

3.1.1 Discretionary access control (DAC) model:

DAC is the traditional access control mechanism in which complete control of all the programs and resources is given to the user. DAC performs access control on the basis of user identity and authorization. It is the mechanism which controls who can access what. In this mechanism, owner of the resource decides the access permission to the user. DAC basically deals with Inheritance of permissions, Auditing of system Events, User Based Authorization and Administrative privileges.

Disadvantage of DAC:

This mechanism is less effective because it can be easily attacked by untrusted third parties and there might be the chance to steal the copy of original message without owner's permission.

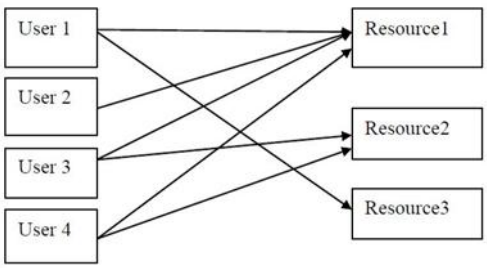

Fig.1. DAC model [4]

3.1.2 Mandatory access control (MAC) model:

MAC is mainly concerned with confidentiality of information. MAC is under control of a security policy administrator. Hence users do not have the ability to override the policy. This policy takes decision based on configuration of network. Each object present in cloud environment assigned some security level.In cloud environment; for each object some security level is assigned. This security level helps to identify the object's current access state.

Advantages of MAC: This mechanism helps to increase integrity of the information and also checks whether the flow is

from high objects to low objects or not. It is mainly used in military, government applications, etc .

Disadvantage of MAC: The security level will not be modified when it is identified to particular subject in hierarchy.

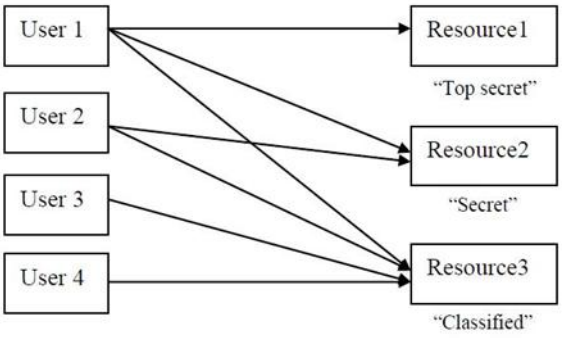

Fig.2. MAC model [4]

3.1.3 Role-based access control (RBAC) model:

Here roles of the individuals and responsibilities are used to provide access policies. It identifies the user role and based on the role it controls the access of a user. Role is a group of policies or objects related to the subject. It may vary from user to user. RBAC provided web based application security. Multiple execution of roles at the same time is allowed to the users. RBAC decides what permission should be assigned to which user.

Advantages of RBAC: it minimizes the damage of information by intruders. User are classified on the basis of their roles.

Disadvantage of RBAC: Based on the privilege of role change; permissions associated with each role can be deleted or changed.

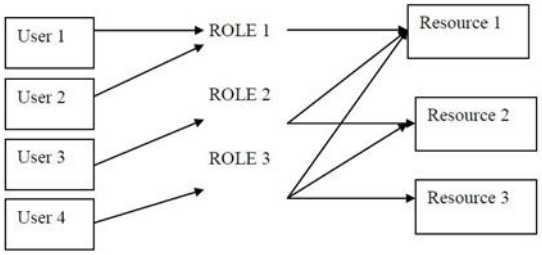

Fig.3. RBAC model [4]

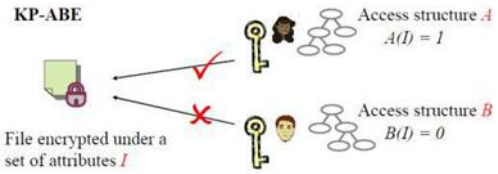

Fig.4. KP-ABE model [5]

3.2.2 Cipher text Policy Attribute based Encryption (CP- ABE):

CP-ABE is revised form of ABE introduced by Sahai [5]. CP-ABE is useful for encrypting data which can be kept confidential even if the storage (proxy) server is not a trusted party. A random number of attributes which are expressed as strings is used as a key for encryption. Whereas, when a data owner encrypts a message he/she designate an associated access structure or access policy over attributes. If the attributes of users who tries to access attributes pass through the access policy defined over cipher text then only user can be able to decrypt the cipher text.

Advantages of CP-ABE: It overpowers the short come of KP-ABE of choosing who can decrypt the data. In CP-ABE user's private key is a mixture of a set of attributes. Hence a user can only use this set of attributes to satisfy the access policy for the particular file.

3.2 Attribute-based encryption (ABE) model:

ABE model was proposed by Sahai and Waters[4] in 2005 year. ABE is the mechanism in which users are allowed to encrypt and decrypt data based on user attributes. User attributes are used to decide the secret key of the user and cipher text. If the set of attributes of the user key matches the attributes of the cipher text; then only decryption of a cipher text is possible. ABE enforces access control through public key cryptography. The central purpose for these models is to provide access control and security. The main aspects are to provide scalability, flexibility and fine grained access control. Considering classical model, this can be achieved only when user and server are in a trusted domain. Another problem with attribute based encryption (ABE) scheme is that data owner needs to use public key of every authorized user to encrypt data. So various ABE based access control schemes have been proposed to overcome this problem.

3.2.1 Key Policy Attribute based Encryption (KP-ABE):

KP-ABE was proposed by Goyal in 2006 which is the extended form of traditional ABE. In KP-ABE cipher text is associated with a set of attributes and decryption key of user is associated with a tree access structure i.e. monotonic. If the cipher text with attributes satisfies the tree access structure, then only user is able to decrypt the cipher text.

Advantages of KP-ABE: The KP-ABE scheme can achieve more flexibility to control users and fine-grained access control than ABE scheme.

Disadvantages of KP-ABE: In KP-ABE scheme, encrypt or cannot decide who can decrypt the encrypted data. Here only descriptive attributes are chosen for data by these scheme. But it is unsuitable in some application because a data owner has to trust the key issuer.

Disadvantages of CP-ABE: CP-ABE is not able to achieve the enterprise necessity of access control which requires accountable flexibility and efficiency. CP-ABE has constraint in terms of specifying access policies and managing every attribute of user. In a CP-ABE scheme, attributes that are organized logically as a single set are supported by decryption keys.

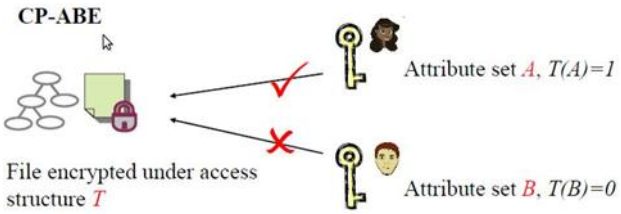

Fig.5. CP-ABE model [5]

3.2.3 Hierarchical Attribute based Encryption (HABE):

The HABE model was derived by Wang et al [6]. HABE model has the hierarchical structure. It consists of root master at the top, which is followed by multiple domain masters that are set of users and users have the set of attributes as shown in the Fig. 6.

Advantages of H-ABE: This scheme fulfills the property of fine grained access control policy, availability and full delegation.

Disadvantages of H-ABE: It is unsuitable to implement H-ABE, because all attributes may be administered by the same domain authority, and hence the same attribute may be administered by multiple domain authorities.

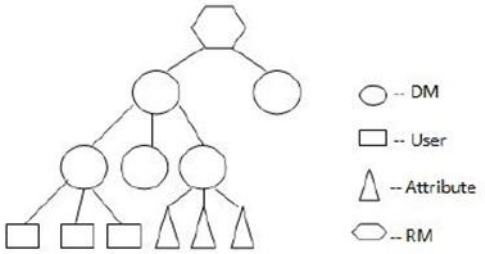

Fig.6. HABE model [4]

3.3 Problem Definition:

Protection of data, i.e. security of data stored in database from unwanted (unauthorized) users or harmful forces. Attribute Based Encryption is an effective security algorithm which creates an unwanted overhead of decryption of cipher text on users and hence, ABE with outsourced decryption was introduced.

Again, outsourcing does not assure the correctness of the decrypted cipher text. Hence, the notion of ABE with Verifiable Outsourced Decryption was proposed wherein the verifiability of decrypted text and original text is done using checksum. We address this scheme in our project.

IV. PROPOSED SYSTEM

The short comes of ABE and ABE with Outsourced Decryption motivate us to study ABE with verifiable outsourced decryption, which we will be implementing in our project. We focus on the context that ABE scheme with secure outsourced decryption does not always assure verifiability (i.e., correctness of the transformation of cipher text done by the proxy server). In this project, we first modify the original model of ABE with outsourced decryption to permit for verifiability of the transformations of the cipher text. For implementation, we have considered a scenario for an IT based firm, wherein the employees of the firm can upload (store) and access documents through a website. The security for this website while uploading and accessing the documents is provided through ABE with verifiable outsourced decryption. Whenever an employee wants to store a file, he uploads it on the server and defines an access policy for the file. This access policy helps in controlling the users who can access the file. The access policy is based on attributes such as *location*, *designation*, *project_id*, etc. Implementation of above scenario can be done using following algorithms:

Our new CP-ABE scheme consists of the following algorithms:

1. Setup(): Produces public key parameters and secret key.
2. Keygen(): Generates private key and transformation key for user.
3. Encrypt(): It uses public parameters, message and access policy to produce cipher text.
4. GenTKOut(): Uses public key parameters,private key and produces transformation key and corresponding retrieving key.
5. Transformout(): It uses public parameters, cipher text, transformation key and provides partially decrypted ciphertext.
6. Decryptout(): It uses public key parameters ,cipher text,partially decrypted cipher text and retrieving key and produces final decrypted message.

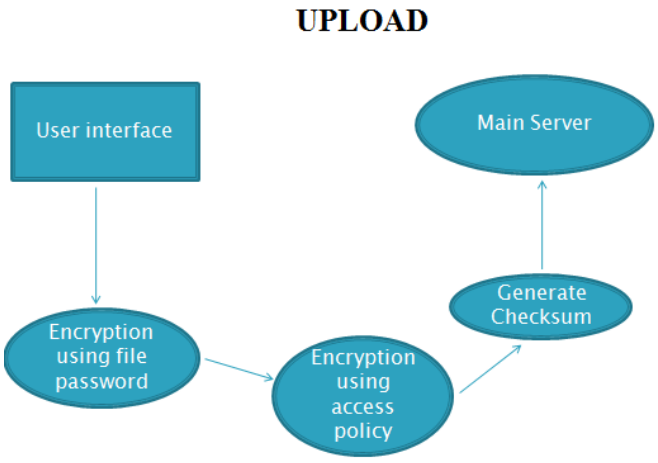

Fig.7. Upload Process

The upload process involves following steps-

Initially when the user uploads a file, he defines an access policy. The system encrypts that file using the file password and also, performs second encryption using the access policy defined by the owner of the file. Alongside it generates the checksum and stores the encrypted checksum along with file in

the main server. The user is unaware about the processes of backend.

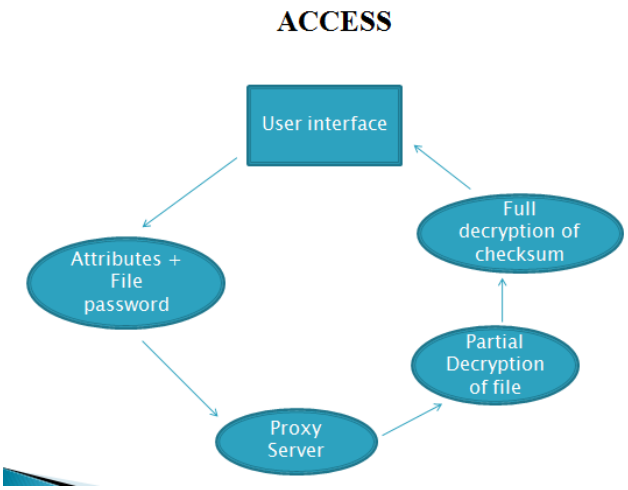

Fig.8. Access Process

In the access process, the user who wants to access the file is asked for the attributes as per the access policy defined by the owner. If the attributes of the user matches the access policy, ie. If the access policy is satisfied then the system performs first decryption using access policy with the help of proxy server. Also the checksum is decrypted. This partially decrypted file is with the proxy server. Now the proxy server asks for the file password from the user. If the file password is correct then the second decryption is performed and the fully decrypted file and checksum is sent to the user. The user's system will now generate the checksum of the received decrypted file and compares it with the received checksum.

Thus, the entire process provides outsourced decryption as well as checks integrity of the file.

V. CONCLUSION

In this paper, we addressed a new requirement of ABE with outsourced decryption: verifiability. We proposed a concrete ABE scheme with verifiable outsourced decryption using a website for an IT firm to store and access documents and thereby proved that it is secure and verifiable. This scheme proved to be more efficient than ABE and ABE with outsourced decryption in every aspect. Also, further improvements can be done by hosting the website on cloud and giving multiple accesses to users.

REFERENCES

[1]https://en.wikipedia.org/wiki/Attribute-based_access_control

[2] http://crypto.stackexchange.com/questions/17893/what-is-attribute-based-encryptionl

[3] http://ijns.femto.com.tw/contents/ijns-v15-n4/ijns-2013-v15-n4-p231-240.pdf

[4]V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encryptdata," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[5]J. Bette ncourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[6]Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012

[7] 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 Proc. EUROCRYPT, 2010, pp. 62–91.

[8]M.Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco

[9] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted worker.