ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 12, December 2013

Secure Attribute Based Mechanism through Access cipher policy in Outsourced Cloud Data

V.Abinaya
PG Scholar
Kalasalingam Institute of Technology
Krishnankoil.

V .Ramesh
Assistant professor
Kalasalingam Institute of Technology
Krishnankoil.

ABSTRACT:

Attribute-based encryption (ABE) is a standard encryption that allows users to encrypt and decrypt data based on user attributes. I t is extension o f attribute set based encryption to improve scalability and flexibility w hile at the same time Inherits the feature of fine grained access control of ABE.It is flexible access control of encrypted data stored in the cloud. It is using access polices and attributes associated with private keys and cipertext. The drawbacks of this scheme are that decryption involves expensive pairing operations. It does not guarantee the correctness of transformation done by the cloud. We consider a new requirement of ABE with outsourced decryption: verifiability. This verifiability used guarantees that a user can efficiently check if the transformation is done correctly. The HMAC algorithm is used to verify data integrity process. In this research focuses on secure and verifiable. The main aim of this paper is without relying on random oracles.

Keywords: Attribute-based encryption, Access control, cloud storage, outsourced decryption, verifiability.

I. INTRODUCTION

ABE is a new vision of public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and cipher texts. There are two kinds of ABE schemes:

- Cipher text-policy ABE (CP-ABE).
- Key-policy ABE (KP-ABE)

In a CP-ABE scheme [8], [9], [5], [6] each cipher text is associated with an access policy according to the attributes. The user's private key is associated with a set of attributes. This user is able to decrypt a cipher text. If the set of attributes associated with the user's private key satisfies the access policy.

In a KP-ABE Scheme [2]–[7] the parts of a quality set and a right to gain entrance strategy are swapped from what we depicted for Cp-Abe: ascribes sets are utilized to clarify the figure writings and access polices over these qualities are connected with user's private keys.

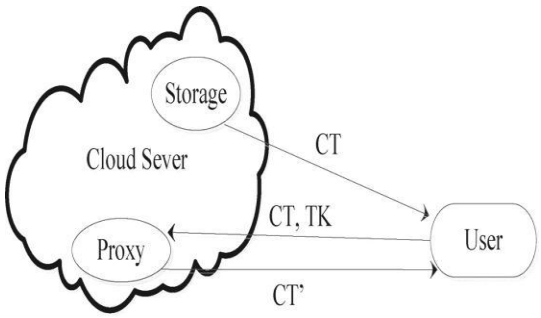


Fig 1: ABE system with outsourced decryption.

In the fig[1] it refers a user provides an untrusted server, say as a proxy operated by a cloud service provider, with a transformation key TK that allows to translate any ABE cipher text CT satisfied by that user's attributes or access policy into a simple cipher text CT'.The small overhead for the user to recover the

plaintext from the transformed cipher text CT'.The drawbacks of the ABE schemes is that number of pairing operations required to decrypt a cipher text Eliminates the decryption overhead for users. The scheme provides no guarantee on the correctness of the transformation done by the cloud server. Our scheme we introduced new method attribute based grows with the complexity of the access policy. The problem by introducing the notion of ABE with outsourced decryption, which largely encryption with outsourced decryption using verifiability. The verification process is used to guarantee data transformation done in cloud.

II. Related Work

Proxy Re-Encryption: In this process perform how todelegate (in a true offline sense) the ability to transform an ABE cipher text on message m into an El Gama style cipher text on the same m, without learning Anything about m. It is similar to the concept of proxy re-encryption. Where an untrusted proxy is given a re-encryption key that allows it to transform an encryption under Alice's key of m into an encryption under Bob's key of the same m, without allowing the proxy to learn anything about m.

Pairing Delegation:It enables a client to outsourcethe computation of parings to another entity. However, the schemes proposed in [15], [16] still require the client to compute multiple exponentiations in the target group for every pairing it outsources. Most importantly, when using paring delegation i n the decryption o f ABE cipher texts.

Linear Secret Sharing Schemes

A secret-sharing scheme [4][6] over a set of parties P is called linear (over Zp) it follows,

1. The shares for each party form a vector over Zp.
2. There exists a matrix an M with l rows and n columns called the share-generating matrix For all I = 1,...., l the i'th row of M .we let the function þ denoted the party labeling row i as þ(i). When we consider the column vector v = (s, r2,....r_n), where s € Zp is the secret to be shared, and r2….. r_n €Zp are randomly chosen. Then (M)v is the vector of (l) shares of the secret s according to π. The share (Mv) i belongs to party þ (i).

III. Cipher text-Policy Attribute Based Encryption

A cipher text-policy attribute based encryption [8] scheme consists of four algorithms:

- Setup
- Encrypt
- KeyGen
- Decrypt.

Setup (ƛ, U): The setup algorithm takes securityparameter and attributes universe description as the input. The outputs take as public parameters (PK) and a master key (MK).

Encrypt (PK, M, A): The encryption algorithm takesas input the public parameters (PK), message (M), and an access structure (A)over the universe of attributes. The algorithm will encrypt (M) and

Bilinear mapping

The bilinear map is a function that combining elements of two vector spaces to yield an element of a third vector space that is linear in each of its arguments.

It reduces the problem of discrete algebra on an elliptical curve to the problem of discrete algebra in a finite field, thereby reducing its complexity. This method has been used an encryption tool for information protection, instead of an attacking tool. Bilinear pairing is equivalent to a bilinear map.

Characteristics that satisfy a bilinear map are as follows.

• **Bilinear**: Define a map e = G × G -> GT as bilinearif e(aP, bP) = e(P, Q)ab, where all P, Q € G, and all a, b € Z.

• **Non-degenerate**: The map does not relate all pairs inG× G to the identity in GT. Note that G and GT are groups of prime order, which implies that if P is a generator of G, e(P, P) is a generator of GT.

•**Computable**: To compute e(P, Q) for any P, Q € G. produce a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. The cipher text implicitly contains A.

Key Generation (MK, S): The key generationalgorithm takes as input the master key (MK) and a set of attributes S that describe the key. It outputs a private key (SK).

Decrypt(PK,CT,SK):The decryption algorithm takesas input the public parameters (PK), a cipher text CT, which contains an access policy (A), and a private key (SK), which is a private key for a set (S) of attributes. It is the set S of attributes satisfies the access structure (A) then the algorithm decrypts the cipher text and return a message M.

IV. CP-ABE Scheme with Verifiable Outsourced Decryption:

The data owner of storage information encrypts the data before outsourcing and it stores at the server. The data owner and users with knowledge about the key will be able to decrypt the data according to attributes. The access of authorizations is to be enforced by the owner. To address the problem of enforcing selective access on outsourced data without need of involving the owner in the access control policy. The goal of is to translate an authorization policy to be enforcing in an identical encryption strategy directed which information are encoded with which key and regulating key release to users. In fig[2] perform the outsourcing decryption process.

Outsourcing decryption resulted in significant practical benefits. Decrypting on an ABE cipher text

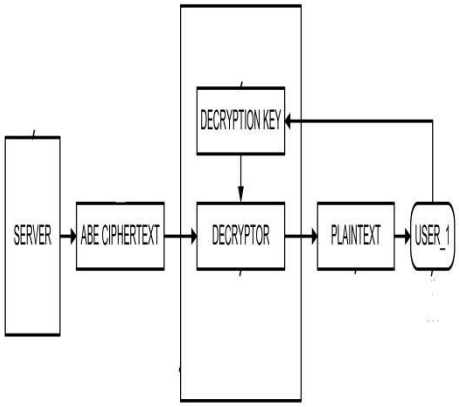


Fig2: outsourcing scenario

Calculation efficiency: The relatively simple pairing calculation implies that the proposed method allows users to generate index and search documents, re-encryption, which increases the calculation efficiency.

containing 100 attributes, we found that without the use of a proxy the mobile device would require about 30 seconds of computation time and drain a significant amount of the device's battery. When we applied our outsourcing technique, decrypting the cipher text took 2 seconds on connect with Intel server and approximately 60 milliseconds on the mobile device itself. In our outsourcing solution, most of this code is pushed into the untrusted transformation algorithm, leaving only a much smaller portion on the user's device. It have some advantages. The decryption code that needs to reside on a resource constrained user device will be smaller. Actually, all bilinear map operations can be pushed outside. This partition will dramatically decrease the size of the trusted code base, removing thousands of lines of complex parsing code. Even without using outsourcing, this partitioning of code is useful

Analysis:

This method to satisfy the following requirements.

• **Confidentiality**: It using pairing, the proposedmethod makes it difficult for a malicious third party to decrypt communication contents, even if they eavesdrop on communications between the client and the server.

• **Search speed**: The user can check whether adocument contains keywords by perform single pairing calculations, which increase the searching speed.

• **Traffic efficiency**: Keyword search and re-encryption requires only one round of communication, so the method increases the communication volume efficiency.

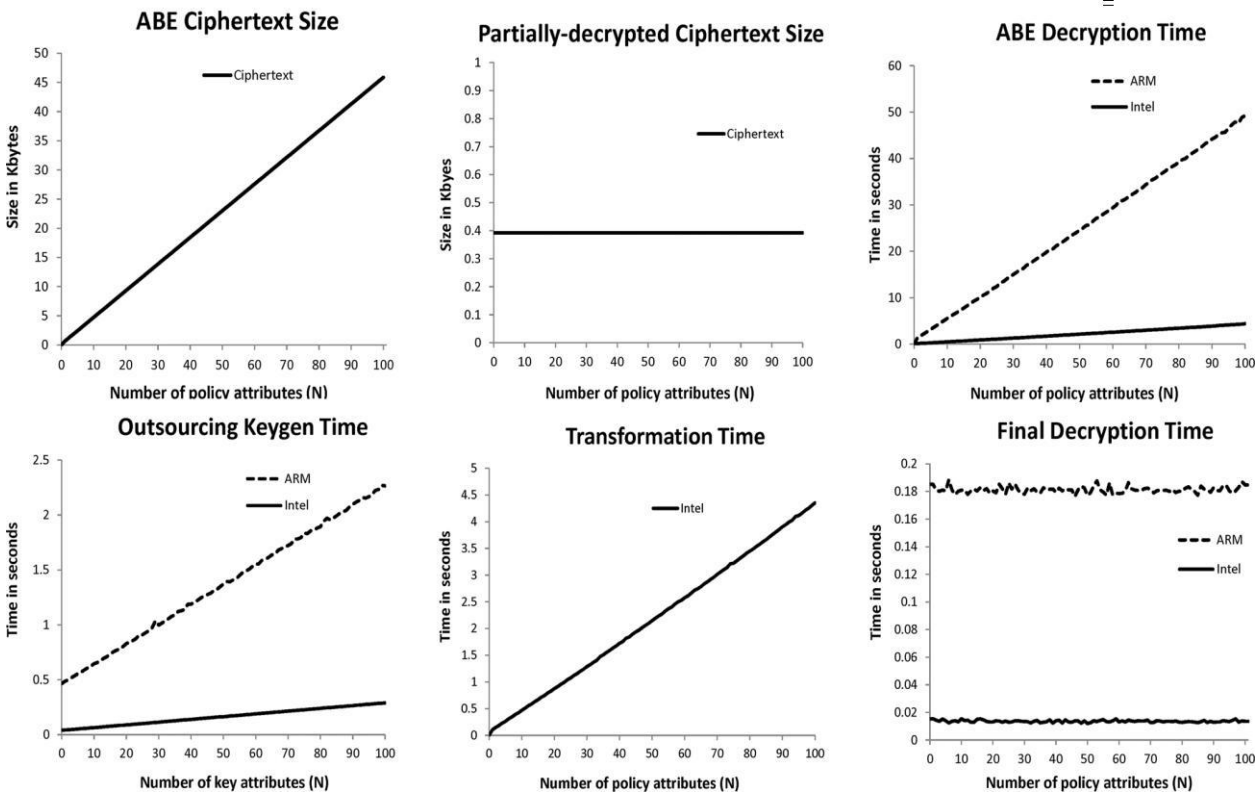
• **Sharing efficiency among users**: Our scheme allows encrypted and stored data on an unreliable distant storage outsourcing server to be shared safely and efficiently. In addition, our proposed method is different from existing methods because it does not require the shared subjects to be specified in advance, and no additional devices are required to manage the subjects who receive the shared data.

V.PERFORMANCE EVALUTION:

In order to evaluate the performance of our CP-ABE scheme with verifiable outsourced decryption [10][11] presented in fig2.We implement our schemein software based on using a 224-bit MNT elliptic curve from the Stanford Pairing-Based Crypto library

Although our implementation based the MNT curve implies the use of asymmetric pairing, only a small change need to be made on our scheme of symmetric setting in the implementation. Specifically, suppose that an asymmetric pairing takes elements from G1 and G2 input.

=



Fig[3]. Performance of our CP-ABE scheme with verifiable outsourced decryption.

VI .CONCLUSION:

We considered a new requirement of ABE with outsourced decryption: Verifiability. It is used to modify the original model of ABE with outsourced Decryption. This ABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .Our scheme does not rely on random oracles. A flexible access control for encrypted data stored in cloud is provided .It eliminates Decryption overhead for users according to attributes .This Data transformation is guaranteed to store in cloud. This secure attribute based cryptographic technique for robust data security that's being shared in the cloud .We enhance the data security process by ABE outsourced decryption technique using Blowfish algorithm.

VII. FUTURE ENHANCEMENT:

To provide Usage of High security cryptographic Using Blowfish algorithm, which is 448 bits key length results in higher security, rather than using traditional DES and AES algorithms are smaller in key sizes results in lesser security. Data Integrity Checking. 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.

REFERENCES:

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc.EUROCRYPT*, 2005, pp. 457– 473.

V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf.Computer and Communications Security*, 2006, pp.89–98.

[3] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Computer andCommunications Security*, 2007, pp. 195–203.

[4] B. Waters, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Public KeyCryptography*, 2011, pp. 53–70.

[5] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, Waters, "Fully secure functional encryption: Attribute based encryption and (hierarchical) inner product encryption," in *Proc.EUROCRYPT*, 2010, pp. 62–91

[6] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the

[11] M. Green, S. Hohenberger, and B. Waters, Outsourcing the decryption of ABE ciphertexts," in *Proc. USENIX Security Symp*, San Francisco, CA,USA, 2011.

[12] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. ACM Conf. Computer andCommunications Security*, 1993, pp. 62–73.

[13] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited (preliminary version)," in *Proc. STOC*, 1998, pp.209–218.decisional linear assumption," in *Proc. CRYPTO*, 2010, pp. 191–208.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute- based encryption," in *Proc.IEEE Symp. Security and Privacy*, 2007, pp. 321–334.

[8] L. Cheung and C. C. Newport, "Provably secure cipher text policy ABE," in *Proc. ACM Conf.Computer and Communications Securit*2007, pp.456–465.

[9] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu "Attribute-based encryption schemes with constant-size ciphertexts," *Theor.Comput. Sci.*, vol. 422, pp. 15–38, 2012.

[10] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. Public KeyCryptography*, 2013, pp. 162–179.

[14] J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in *Proc. CRYPTO*,2002, pp. 111–126.

[15] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc.CRYPTO*, 2010, pp. 465–482.

[16] B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairing computation," *IACRCryptology ePrint Archive*, vol. 2005, p. 259,2005.

First Author Ms.V.Abinaya
The author is currently a ME Student in Computer Science and Engineering Department at Kalasalingam Institute of Technology.She had completedBE from Kalasalingam University.

Second Author Mr. V.Ramesh
The author is an Assistant Professor in Computer Science Engineering Department at Kalasalingam Institute of Technology. He received his BE from Syed Ammal Engineering College; affiliated To Anna University, and M.Tech. Degree from Kalasalingam University. His Research interests are in the areas of network security, Data Mining and cloud computing Security