ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure and Efficient Cipher Text Policy Attribute Based Encryption without Key Escrow Problem

D.Ujwal
PG Scholar,
Department of CSE,
Aurora's Scientific Technological & Research Academy.

S.Shalini
Assistant professor,
Department of CSE,
Aurora's Scientific Technological & Research Academy.

Abstract:

Attribute Based Encryption with Verifiable Outsourced Decryption is a challenging application that server public key based one to many encryption that allows the user for the encryption and the decryption of the file/ data based on his own attributes. This application also server the user in terms of security saying no malicious cloud will be able to learn about the encrypted file and also provides fully security against the key being compromised by the cryptanalyst. ABE with Verifiable Outsourced Decryption also introduces Verifiability with the use of Checksum that will be generated by the user.

Keywords: ABE,CP-ABE,KP-ABE,CT,MK,SK

1.INTRODUCTION:

Attribute Based Encryption with Verifiable Outsourced Decryption is a public key based one to many encryption, in which the encrypted content that is known as cipher-text is associated with the access policy and the attributes what user uses to encrypt the data is associated with the Private Key. The two schemes that are associated with the Attribute Based Encryption is:

1)Cipher-Text Policy Attribute Based Encryption. (CP-ABE).
2)Key Policy Attribute Based Encryption. (KP-ABE).

In this application we are using only Cipher-Text policy attribute based encryption where the user will encrypt the file using the private key that is nothing but the personal details of the user which will be served as an attributes. Later, for the decryption purpose the Access Policy plays a vital role. The access policy is the sentence formation by using all the attributes of the user that he uses to encrypt the data. Once if the access policy is matched with the attributes only then the user is an authorized user and will be able to decrypt the data that will be sent by the server.

ABE also introduces the intermediate server known as the proxy server that plays a vital role in reducing the work load of the main server. The user once he encrypts the file, the file will be stored in the server. User once in need of file will request to the intermediate server that is proxy server and the proxy server will in turn send the user details to the server and will ask the server to check whether the user is the authorized user or not. Based on the reply of the server, proxy server will takes the further action. If the user is an authorized user the server sends the reply as an authorized user, once getting the reply as such, the proxy server will request the user to send the transformation key. By using the transformation key the proxy server will partially decrypts the file that will be known as transformed cipher-text.

The transformed cipher-text is than sent to the user for the complete decryption where the plain text will be generated. As the proxy server is the transparent server there are chances of proxy server taking the wrong file or taking the correct file with the wrong information in it on the request of the authorized user. To eliminate this we are using the checksum, which verifies whether the file that was encrypted and stored to the server and the file that is been received through the proxy server for the partial decryption that is the transformed cipher-text is the same.

Attribute Based Encryption with Verifiable Outsourced Decryption gurantess the security property that no malicious cloud will be able to learn anything about the encrypted data. One of the demerit that is related to the existing scheme of ABE is, for resource limited devices the decryption is very expensive due to pairing operation. The complexity of pairing operation increases with the increase in the access policy and the compexity of the access policy increase with the increase in the user attributes. As so further, let me take the example for both resource limited device such as any hand held device ex: Mobile Phone and on the comparission of it any Intel Processor.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Now, if suppose the file is decrypted from the handheld device in the absence of proxy, the same device will take almost 50 seconds for the standard decryption where in it takes only 5 seconds for the Intel Processor. By introducing the proxy server we are reducing the burdensome task of the handheld device which results in the less computation cost of the mobile device. The mobile device which early took 50 seconds for the standard decryption will now be able to decrypt the same file with approximately 180 milliseconds.

2.CIPHER POLICY ATTRIBUTE BASED ENCRYPTION

Thus the cipher text-policy attribute based encryption scheme consists of four algorithms:

•Setup
•Encrypt
•Key Gen
•Decrypt

Setup (λ, U)
The setup algorithm takes security parameter and attributes universe description as input. It outputs the public parameters (PK) and a master key (MK).

Encrypt (PK, M, A)
The encryption algorithm takes as input the public parameters (PK), a message (M), and an access structure A. It outputs a cipher-text CT. Key Generation (MK, S) The key generation algorithm 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 takes as input the public parameters (PK), 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. If the set (S) of attributes satisfies the access structure A then the algorithm decrypt the cipher text and return a message
(M)

3.VERIFIABILITY :

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

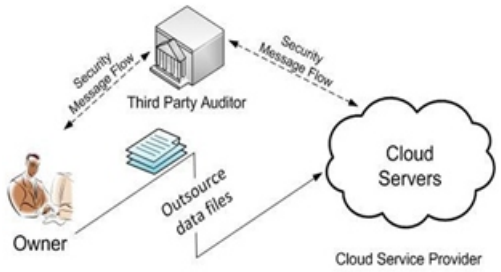
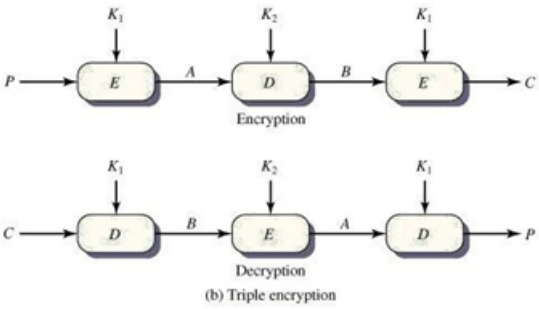


Fig: Cloud Storage Verification

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.



(b) Triple encryption

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 proves the strength of algorithm when used key options 2 and provides backward compatibility with DES with key option 3.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 ie 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.The key option 3 provides backward compatibility with DES.

4 .RELATED WORKS

Sahai and Waters[1] have also addressed the issue by introducing the notion of attribute based encryption.Green et al[12] have proposed the secure attribute based encryption scheme with outsourced decryption, but this was not verifiable.

5. ANALYSIS

This method satisfies the following requirements.

Confidentiality:

As the complexity of the pairing operation increases, it will be very difficult for the malicious thirdparty to read or hack the encrypted content even thought eavesdrop on communication between the client and the sever.

Authentication:

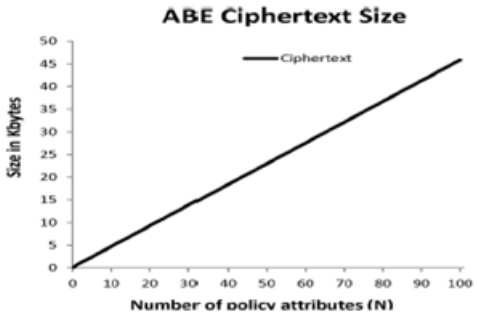
As the document owner's attributes is used as the private key to encrypt the data which also server's aspartial digital signature, as and when the data is decrypted by the data owner, he will be satisfied with the content as he has used his own attribute to encrypt it.

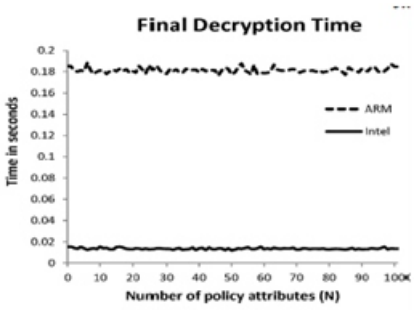
Verifiability:

Check sum is widely used to verify whether the content that is encrypted and the content that is beenreceived by the data owner is same.

Performance Evaluation:

In order to evaluate the performance of CP-ABE scheme with verifiable outsourced decryption is presented in the below figures.





6.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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCE:

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

[2]V.Goyal, O. Pandey,A. Sahai, and B.Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in Proc. ACMConf. Computer and Communications Security, 2006, pp. 89–98.

[3]T. Okamoto and K. Takashima, "Fully secure functional encryptionwith general relations from the decisional linear assumption," in Proc. CRYPTO, 2010, pp. 191–208.

[4]N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-sizeciphertexts," Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.

[5]B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, "Secure delegation of elliptic-curve pairing," in Proc. CARDIS, 2010, pp. 24–35.

[6]B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairingcomputation," IACR Cryptology ePrint Archive, vol. 2005, p. 259, 2005.

[7]G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxyre-encryption schemes with applications to secure distributed storage," in Proc. NDSS, San Diego, CA, USA, 2005.

[8]A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," Ph.D. dissertation, Israel Inst. of Technology, Technion City, Haifa, Israel, 1996.

[9]A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. EUROCRYPT, 2011, pp. 568–588.

[10]N. P. Smart and F. Vercauteren, "On computable isomorphisms in efficientasymmetric pairing-based systems,"Discrete Appl. Math., vol. 155, no. 4, pp. 538–547, 2007.

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