ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Attribute Based Mechanism Using Cipher Policy Verification

[I]V.Abinaya, [II]V.Ramesh
[I]PG Student, Dept. of CSE, Kalasalingam Institute of Technology, Krishnankoil, India
[II]Assistant Professor, Dept. of CSE, Kalasalingam Institute of Technology, Krishnankoil, India

Abstract
Cloud storage enables users to remotely store their data and enjoy the on demand high quality cloud applications without the burden of local hardware and software management. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users. This project proposed an effective Attribute based encryption with verifiable outsourced Decryption. Attribute Based Encryption is a standard encryption that allows users to encrypt and decrypt data based on user attributes. It is flexible access control of encrypted data stored in the cloud. It is using access polices and attributes associated with private keys. The drawbacks of this scheme are that decryption involves expensive pairing operations. It does not guarantee the correctness of the transformation done by the cloud. We consider a new requirement of ABE with outsourced decryption perform verifiability process. This verifiability used guarantees that a user can efficiently check if the transformation is done correctly. The main aim of this project is without relying on random oracles.

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

I. Introduction

In cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Attribute-based encryption (ABE) [2][8] has been envisioned as a promising cryptographic primitive for realizing secure and flexible access control. Process extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. Having Remote database, there arises Security. So, In order to maintain data integrity, proposed design consists of efficient methods that enable on-demand data correctness verification.

Traditional Cloud security concepts ensure the Identity based Cryptography which with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine grained access control of ABE. In order to achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service, In efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed.

Cloud storage service architecture is illustrated by three different network entities. It can be identified as follows:

User: An entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise to on individual customers.

Cloud Server (CS): An entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter).

Public Key Infrastructure: A PKI has one more trusted entity called Certification Authorities (CAs). For example, The VeriSign is a CA.

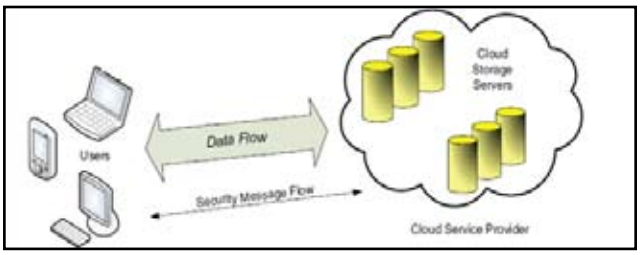


Fig. 1.1: Cloud Storage Services

II. Attribute Based Encryption

In a conventional public key crypto method system, there are two distinct keys:

- Public key
- Private Key.

Bob uses Alice's public key to encrypt a message to Alice. The Alice uses her private key to decrypt the message. The Alice may have given the public key using a secure communication channel along with user attributes. This works only if there is already some trust the familiarity between both Bob and Alice. In an unknown open system, we need a trusted third party (TTP) to uniquely bind public keys to users or another entity such as an organization.

Here we need a PKI (Public Key Infrastructure). A PKI has one more trusted entity called Certification Authorities (CAs). For example, VeriSign is a CA. CA issues Alice a certificate (which contains the public key of Alice) signed by the CA's public key after verifying Alice's credentials message. Now Bob can now retrieve Alice's certificate and verify it is authentic by checking the signature on it.

Some smart researchers came up with the idea of using user identities (for example, your email address) as public keys. Such systems are called IBE (identity based encryption). Notice that there is a huge trust placed on the KGS (Key Generation Security). The security of the whole system relies on the security of the KGS and how well the KGS authenticates users before issuing private keys. The idea of IBE [1] was further improved to support much better systems. ABE can be considered as a generalization of identity based encryption (IBE).where, as mentioned the encryption is based on some identity. ABE[5][6] is a new vision of public key based one-to-many encryption that enables access control over encrypted data using access policies.

A. 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 over the universe of attributes. The algorithm will encrypt (M) and 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.

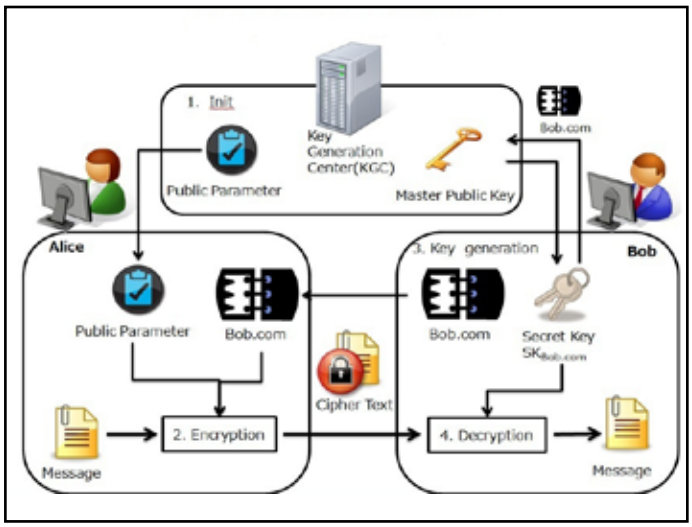


Figure 2.1: key generation using Attribute Based Mechanism

In figure 2.1 shows key generation of ABE is more expressive than the IBE. In an ABE [7][9] system, the plaintext is encrypted with a set of attributes. In the KGS, which possesses the master key, issues used different private keys to users. In basic form, a user can decrypt a cipher text if and only if there is a match between the attributes of the cipher text and the user's key.

1. 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).

2. 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. Bilinear mapping process

Bilinear is a function combining elements of two vector spaces to yield an element of a third vector space that is linear in each of its arguments. It is mapping two file attribute generate public key using to perform encryption process.
Characteristics that satisfy a bilinear map are as follows.

• Bilinear: Define a map e = G × G -> GT as bilinear if 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 in G× 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.

III. Verifiability Process

In figure 3.1 shows Data retrieved from the server, it needs to be checked whether the received data is valid or not. Data storage correctness [3][4] is more significant besides secured outsourcing of data in cloud. Data owner has to audit or verify data integrity of received data from the cloud server. Data owner used HMAC algorithm which is Hash-Based Message Authentication Algorithm for the verification of the data being received from the cloud.

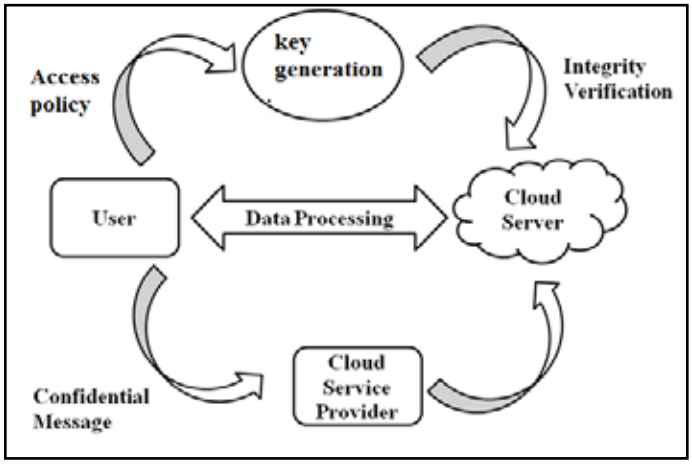


Figure 3.1: Cloud Storage Verification

A. Data security algorithm

1. Blow Fish Algorithm

Blowfish has a 64-cycle piece measure and a variable key length from 32 bits up to 448 bits and making it perfect for securing information.
It is a variable-length key for block cipher encryption process her method . It is suitable for applications where the key does not change often, like a communications link of an automatic file encryption method. It is a symmetric piece figure that might be utilized as a drop-in supplanting for DES or IDEA. It was planned as a quick, free elective to existing encryption calculations. It has been broke down impressively, and it is gradually picking up acknowledgement as an in number encryption. It is much quicker than DES and AES. It is suitable and productive for equipment execution. Also, it is unpatented and no permit is needed. Blowfish has been liable to a lot of cryptanalysis method and full Blowfish encryption has never been broken.

B. Data Integrity Algorithm

1. MAC [Message Authentication code]

Message Authentication Codes (MAC) is a method in which the integrity of data is checked using secret key that is shared between a sender and a receiver. This method can also apply to a single sender sending data to multiple recipients. The Message Authentication Code standard is a cryptographic checksum that results from passing data through a message authentication algorithm along with user attributes. Generally, this means that the message authentication codes are used between senders and receiver that share a secret key to validate the information being transmitted. In spite of the fact that the MAC strategy is robust, because of the advancement of sniffer and bundle catching provisions.
A message digest algorithm takes a single input a message and

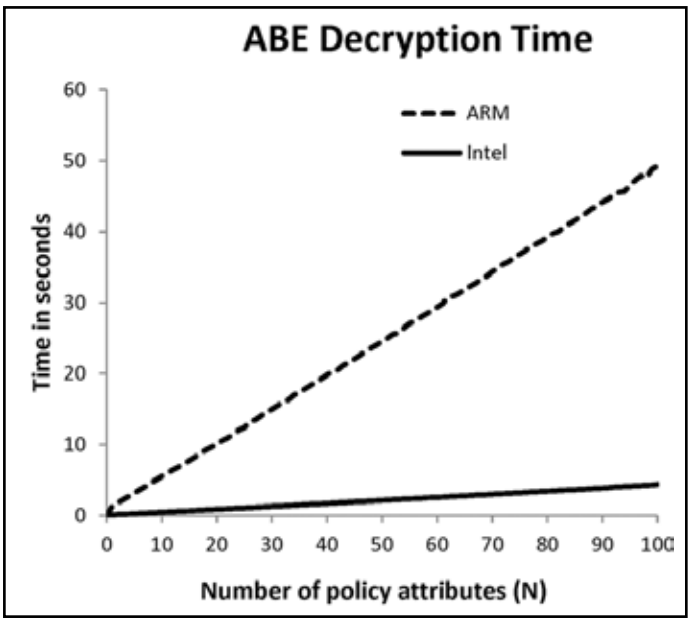
ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

produces a "message digest" which allows you to verify the integrity of the message: Any change to the message will (ideally) result in a different hash being generated. The attacker that can replace the message and digest is fully capable of replacing the message and digest with a new valid pair.

A MAC algorithm takes two inputs: message and secret key. It produces a MAC which allows you to verify the integrity and the authenticity of the message: Any change to the message or the secret key will (ideally) result in a different MAC being generated .It does not without access to the secret should be able to generate a MAC calculation that verifies; in other words a MAC can be used to check that the MAC was generated by a party that has access to the secret key.

IV. Performance Evalution

In order to evaluate the performance of our CP-ABE scheme with verifiable outsourced decryption presented in figure [4.1]. We implement our scheme in software based on using a 224-bit curve from the Stanford Pairing Based Crypto library. Only a small change needs 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.



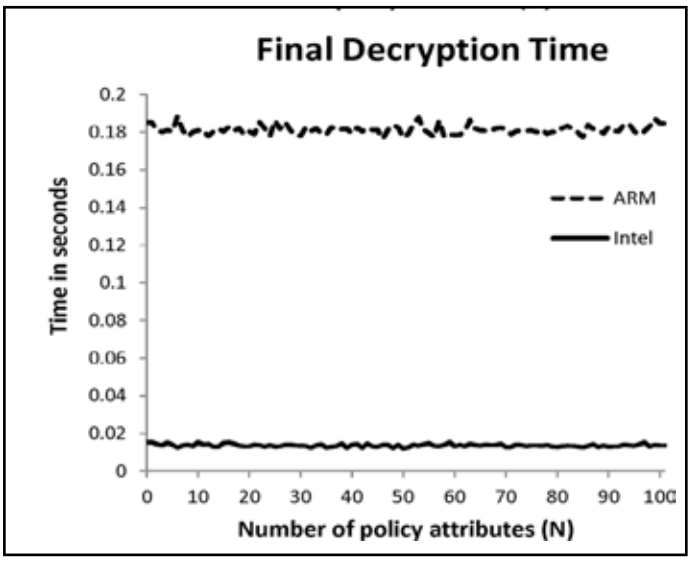


Figure 4.1: Performance of CP-ABE scheme

V. Conclusion

In which considered a new requirement of ABE with outsourced decryption verifiability. 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 secures attribute based cryptographic technique for robust data security that's being shared in the cloud We enhances the data security process by ABE outsourced decryption technique using Blowfish algorithm.

VI. Future Enhancement

To provide Usage of High security cryptographic 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.

References

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

[2] *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*

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

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

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

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

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

[8] *B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairing computation," IACR Cryptology Print Archive, vol. 2005, p. 259.*

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

[10] *B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairing computation," IACR Cryptology ePrint Archive, vol. 2005, pp. 259.*

Ms.V.Abinaya, the author is currently a ME Student in Computer Science and Engineering Department at Kalasalingam Institute of Technology. She had completed B.TECH from Kalasalingam University.

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