

“Key-Policy Attribute-Based Encryption with Equality Test in Cloud Computing”

Sayali Shirishrao Deshmukh, Prof. Dharashive N.G.

*Dept. Of computer engineering,
M. S. Bidve Engineering College, Latur*

Date of Submission: 20-08-2022

Date of Acceptance: 31-08-2022

ABSTRACT

Privacy of data is an important concept while we are uploading, downloading data on the cloud. The term cloud computing are adopted widely in daily life and industrial production. Many individuals and companies are motivated to outsource their data and services to clouds. When user wants to put or save his/her confidential data on cloud he/she encrypts the sensitive data under an access policy and also build a secure index for the set of keywords. The concept of Public-key encryption with keyword search (PEKS) is convenient for users to use the data without leaking privacy. Concept of Public-key encryption with keyword search (PEKS) is convenient for users to use the data without leaking privacy. Public key encryption algorithm which supports plaintext equality test and user-specified authorization. Here public key encryption with equality test is concatenated with key-policy attribute-based encryption (KP-ABE) to present key-policy attribute-based encryption with equality test (KP-ABEwET). Key policy attribute based encryption is an important cryptographic primitive for user's outsourced data. In this paper we proposed the system for preventing the confidential information of user with the concept of Equality test and public key encryption.

The concept of Diffie Hellman algorithm is used for key exchange in public network. In this technique two parties that have no prior knowledge of each other who jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Keywords: Cloud computing, Encryption, Public key encryption, Equality test, Attribute based encryption

I. INTRODUCTION

The concept of public key encryption is widely used in the case of providing security. It is the scheme where large number of values used to

encrypt the data. So this concept is useful while storing user confidential data or information. Key policy attribute base encryption is the scheme where plaintext and cipher text terms are used. While cipher text term is used by sender with set of descriptive attribute set while private key is issued by trusted party. This scheme is suitable for structured organization which follows rules about who may read the document. The recommended system uses the term equality test to check whether two cipher texts contain same text after decryption. To provide more accurate encrypted data attribute based encryption is used. So with the help of key policy attribute based encryption is a scheme we can store sensitive data on cloud safely.

To provide more security to our data here we use policy based encryption. It means set of rules which are used to design emails and to encrypt any email based on predefined conditions. With the help this concept key policy attribute based encryption enable sender to decrypt the message under the set of some rules and attributes. Private key is the concept of encryption mechanism that specifies the key in which cipher text can hold will be allowed to decrypt the messages. Equality test of strings is the term used to check two strings or data entered by user. By using the concept of equality test we can check two different cipher text contains the same message.

The concept of public key encryption search can perform keyword searches over cipher texts without decrypting them. Data confidentiality and privacy is a set of rules that protects a certain type of information by placing some restrictions on it. It is an essential requirement for cloud storage since the cloud service provider, which stores the data, is normally unauthorized to access its content.

KP-ABE is the mechanism which uses users' secret keys generated based on an access tree that defines the privileges scope of the concerned user and data are encrypted over a set of attributes.

Cipher text policy attribute-based

encryption is the mechanism associated with the access policy and the encrypting party determines the policy under which the data can be decrypted, while the secret key is associated with a set of attributes.

Scheme used:

Encryption: It is the concept of converting secret code into information which is hard to understand. Confidentiality is the main term in which concealing the content of the message by translating it into a code.

To encrypt the data complex mathematical algorithms and digital keys to encrypt data.

Decryption: It is the concept of conversion of encrypted data into its original form. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.

Public key cryptography: This is a concept or method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use.

II. LITERATURE SURVEY

D. Boneh G. D. Crescenzo, R. Ostrovsky, and G. Persiano proposed key-policy attribute-based encryption (KP-ABE) in 2004. They said that the underlying cryptosystem combines the secret key and the access structure.

Bethen court et al. proposed cipher text policy attribute-based encryption (CP-ABE) in 2007, which combines the cipher text and the access structure.

New cryptosystem called public key encryption with equality test (PKE-ET) has been introduced in 2010. This proposed system can test whether two cipher texts contain the same plaintexts without decryption.

Amit Sahai stated that a user's private key will be associated with an arbitrary number of attributes expressed as strings. When a party encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure.

Yang et al presented a new cryptosystem called public key encryption with equality test (PKEwET). His proposed system can test whether two cipher texts contain the same plaintexts without decryption. However, this scheme allows anyone to perform such a test.

Sahai, and B. Waters Proposed a key-policy attribute-based encryption(KP-ABE) scheme. It is the modified form of classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is

associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data.

To protect data, confidential information, data security and privacy and different encryption technique in keyword search Changji Wang, Wentao Li, Yuan Li, and Xilei proposed the system A Cipher text Policy Attribute Based Encryption Scheme Supporting Keyword Search Function to support the system.

The sender uses the public key to perform the encryption, but the private key is kept secret from the receiver. This is also known as asymmetric key algorithm.

To define and construct a mechanism that enable user to provide a key to the gateway that enables the gateway to test whether the keyword in the email without learning anything else to test whether the word is a keyword in the email without learning anything else about the email. This mechanism of Public Key Encryption with keyword Search proposed by Giovanni Di Crescenzo.

Public key encryption is a scheme is a public key encryption technique that is designed for one-to-many communications. In this scheme, data is associated with the attributes for which a public key is defined for each.

In cryptography, plaintext is usually ordinary readable text before it is encrypted into cipher text, or readable text after it is decrypted. Data input to or output from encryption algorithms is not always plaintext.

III. WORK FLOW

In this system we combine the concept of public key encryption, equality test and attribute based encryption. We also provide here security model of our scheme. Key policy attribute based encryption with equality test in cloud computing is an extension for attribute based encryption.

Here user enters into the system with username and password. If user is new then he has to login with some data. Then he has to select appropriate option for performing action like upload data, download data, and view data which he already uploaded. Third Party Auditor is the Authorized person in cloud.TPA has a separate authentication in this system, using that TPA will login in to the system. TPA can view the registered user details and also TPA has authorization to provide key for the users.TPA will see the details and provide key to the users.

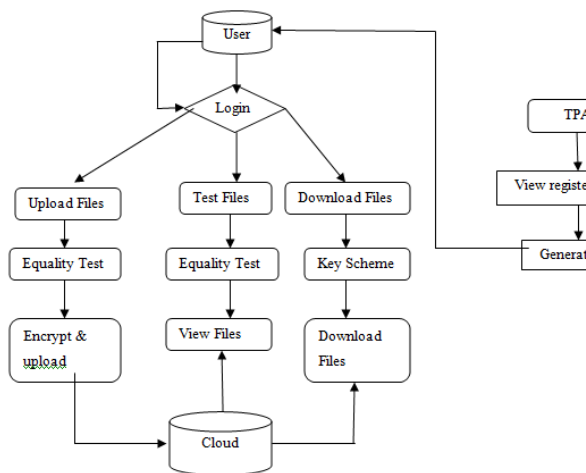
User want to upload files then he first choose file form location. Then he has to send

request to TPA for taking permission from admin, for this task he has to do Equality test. If it matches with the TPA key then only he can upload documents.

file has been uploaded, then user has to test the file whether it is saved correctly. To test file user has to send request to Admin for testing file, again equality test has been performed. If it matches then only user can see file material.

To download data from cloud user have to share his key provided at the time of login from admin, if the key matches then only user can download data from cloud.

User has to test the file whether it is saved correctly. To test file user has to send request to Admin for testing file, again equality test has been performed. If it matches then only user can see file material.



Key policy attribute based encryption with equality test scheme consists of six algorithms.

Setup (k): It takes a security parameter k as input, and then it outputs the public parameters pp and pk and the master key mk.

Encrypt (M, pk, S, S'): It takes a message $M \in \mathcal{M}$, public key pk and two sets of attributes S, S' as inputs, and then it outputs the cipher text $CT \in \mathcal{C}$.

KeyGen (T, T', S, S', pp, mk): This algorithm takes as inputs the master key mk, two access trees T, T', and two sets of attributes S, S' that satisfy $T(S) = 1$ and $T'(S') = 1$, and it subsequently outputs the private key sk.

Trapdoor(S', T', mk): It takes mk, T' and S' as inputs, and it outputs the trapdoor td.

Decrypt (CT, sk, S, S'): It takes as inputs a cipher text $CT \in \mathcal{C}$, S, S' and the private key sk, and it outputs the message M if $T(S) = 1$ and $T'(S') = 1$. Here, CT is encrypted using the sets S and S'.

Test (CT_A, CT_B, td_A, td_B, S'): Suppose that CT_A is a cipher text of the sets of attributes S_A and S'_A and that CT_B is a cipher text of the sets of attributes S_B and S'_B. This algorithm takes as inputs two cipher texts CT_A, CT_B, the trapdoors td_A, td_B and the set S' of attributes that satisfy $T'_A(S') = 1$ and $T'_B(S') = 1$, and then it outputs 1 if CT_A and CT_B contain the same message; otherwise, it returns 0.

Diffie-Hellman key exchange policy:

The Diffie-Hellman is a key exchange protocol which enables the two parties communicating over public network to establish a secret connection without being transmitted over the Internet. Diffie Hellman enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography.

This channel is used by the systems to exchange a private key. This private key is then used to do symmetric encryption between the two systems.

The Diffie-Hellman algorithm was one of the earliest known asymmetric key implementations. The Diffie-Hellman algorithm is mostly used for key exchange.

IV. CONCLUSION

From all the information we can conclude that new scheme provide fine authorization of data security. This scheme is an extension for attribute based encryption to solve the issue of that. Proposed scheme uses Equality test to provide more secure way for hiding confidential information. Security model of authorization is proven in this model.

Key policy attribute based encryption with equality test (KPABewET) is the first attempt to combine the concept of public key encryption that support equality test with attribute based encryption (ABE).

REFERENCES

- [1]. A.Sahai, B. Waters. "Fuzzy identity-based encryption", Annual International Conference on the Theory and Applications of Cryptographic techniques. Springer Berlin Heidelberg, 2005: 457-473
- [2]. "Enhancing privacy using collaborative attribute encryption Techniques", Ansari Tasin Habib Ahmad, Dr. J. W. Bakal, 2016

- [3]. “An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Cipher text Length”, Changji Wang^{1, 2, 3} and Jianfa Luo^{1, 2} march 2013
- [4]. Zvika Brakerski¹ and Gil Segev Better Security for Deterministic Public-Key Encryption, 2011.
- [5]. Amit Sahai, Cipher text-Policy Attribute-Based Encryption, 2007.
- [6]. Dan Boneh¹, “Public Key Encryption with Keyword Search”, 2004.
- [7]. Shengke Zeng^{1,3} “ID-based Encryption with Equality Test against Insider Attack”, 2017
- [8]. Changji Wang^{1,2}, Wentao Li¹, Yuan Li¹, and Xilei Xu¹, “A Cipher text-Policy Attribute-Based Encryption Scheme Supporting Keyword Search Function”, January 2013.