ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(25), DOI: 10.17485/ijst/2015/v8i25/75227, October 2015* ISSN (Online) : 0974-5645

Solitude Conserve Attribute Cryptographic CP-ABFE Data Protocols in Fuzzy Cloud Service Provider

Sreela Sreedhar[1*], Varghese Paul[2] and A. S. Aneesh Kumar[3]

[1]Department of CSE, Toc H Institute of Science and Technology, Ernakulam-682313, Kerala, India; sreelasreedhar@gmail.com.
[2] CS IT/Research, Toc H Institute of Science and Technology, Arakkunnam, Ernakulam-682313, Kerala, India; vp.itcusat@gmail.com
[3]Department of CSE, Alpha College, Porur, Chennai - 600095, Tamil Nadu, India; sreela1234sreela@gmail.com

Abstract

Background/Objectives: Privacy is considered as non-compromising demand of the user in utilities where the user's private and vital information such as user name, user transaction details, user ID, and other specific particulars are used. In this situation the application of conservative cryptographic schemes and unspecified authentications are not enough, and so the implementation of special kind Cipher Text-Policy Attribute-Based Fuzzy Encryption (CP-ABFE) is introduced. It ensures authentication, integrity of communications, data security and user privacy to the consumers on cloud. **Methods/ Statistical Analysis:** We developed a model known as CP-ABFE for providing security for CP-ABE. We made analysis with CP-ABFE scheme. The achieved results show that our module reached with more tedious access controls and hierarchical attributes in Fuzzy Cloud Service Provider. **Results**: The achieved results are used to validate our proposed model and identified that the solution is very efficient and effective in supporting fuzzy encrypted data search over Fuzzy CSP data. **Conclusion/Application**: In this system, a user's private key is associated with an arbitrary number of attributes which uttered as a string. On the other hand, if a party encrypts a message in our system, then that states an associated access construction over the attributes.

Keywords: CP-ABE, Cloud Security, Fuzzy, Fuzzy Encryption

1. Introduction

Cloud systems[1] are extensively adopted and prominent model for delivering services and support over the internet currently. There are large amount of valuable and sensitive data storage on the clouds and so the cloud service providers are in a position to offer confidentiality and security. Cryptographic algorithms are used to ensure this protection, where the data is encrypted before uploading to the cloud. A cryptographic solution for achieving fine grained data access control is Attribute Based Encryption[2]. In this paper, we propose two new secured techniques known as CP-ABFE and Fuzzy Cloud Service Provider Security (FCSPS)[3–5]. CP-ABFE can address the security among different clouds and also reduce the count of required secret keys. The Fuzzy encrypted data will be kept confidentially and securely against collusion attacks. In FCSPS the concept of fuzzy is introduced for a hopeful authority to preserve the integrity of cloud functions in cloud service provider, which is consider as a highly secured file-sharing strategy with better flexibility and scalability of the stored data by modifying Attribute Cipher text-Policy (CP-ABE).

2. Objectives

- To analyze and evaluate contemporary privacy security of CP-ABE.

* *Author for correspondence*

- To determine the security decisions of fuzzy cloud service provider with the presence of computationally connected devices.
- To propose privacy preserving techniques with CP ABE in Fuzzy encrypted data framework.
- To measure the efficiency of developed CP-ABFE's primitives and operations.
- To outline the scrutiny procedure of the proposed framework.

3. Our Contributions

The contributions of this paper are listed below.

- We developed a model known as CP-ABFE for providing security for CP-ABE.
- We made analysis with CP-ABFE scheme.

The achieved results shows that our module reached with more tedious access controls and hierarchical attributes in Fuzzy Cloud Service Provider.

4. Attribute Based Encryption

Attribute Based scheme was introduced by Sahai and Waters in the year 2005 with the objective of proving security and access control. Attribute-Based Encryption (ABE) is a Public-Key based One-to-Many encryption system that allows users to encrypt and decrypt data based on user attributes. The secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold valued. Collusion-resistance is crucial security feature of Attribute-Based Encryption. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

ABE comes in two flavors called Key-Policy ABE (KP-ABE) and Cipher text-Policy ABE (CP-ABE)[6]. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users, keys; while in CP-ABE, the attributes are used to describe users' credentials and the person to encrypt determines a policy on who can decrypt the data. Comparing the two approaches, CP-ABE is more appropriate to the data sharing system because it place the access policy decisions in the hands of the data owners.

5. Cipher Text-Policy Attribute Based Encryption (CP ABE)

In Cipher Text-Policy Attribute Based Encryption (CP-ABE), the user's Private-Key is always associated with a group of attributes and the access policy of cipher text specifies a universe of attributes within the system. In this if the user's attributes satisfies cipher text policy, then the user will be allowed to decrypt a cipher text[7]. The policies in it is designed with conjunctions, disjunctions and (k, n)-threshold gates. For instance, let us assume the universe of attributes as $\{A, B, C, D\}$ and the first user may receive a key to attributes $\{A, B\}$ and the second user may to attribute $\{D\}$. If a cipher text is encrypted with respect to $(A \wedge C) \wedge D$, then the second user will able to decrypt, while the first user can't decrypt[8,9].

CP-ABE follows implicit authorization which provides authorization for encrypted data and allows only the people to decrypt data, if they satisfy associated policy. The important feature is that the user can attain their private key only after the data encryption with respect to the given policies[10].

6. Our Module

We propose an Attribute based fuzzy encryption model that is specified by the encryptor to conserve privacy of the access policy. This scheme is considered as very much significant and probably secured under the Fuzzy Cloud Services Provider. CP ABFE technique can keep the data confidentially and in a secured manner against collusion attacks by using Fuzzy encryption's-ABFE algorithm follows four steps and which are,

- Setup: This algorithm takes an input as a security parameter k and returns the public key PK as well as a system master secret key MSK. PK is normally used by the sender for the purpose of fuzzy encryption. The master secret key, MSK is used for generating user secret keys and it can be identified only by the authority.
- Encryption: This algorithm takes PK, a message M_S, an access tree structure A_T with fuzzy and outputs the cipher text CT.
- Key-Generation: This step uses input set of attributes associated with the user and the master secret key MSK and outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure $A_{T,}$ if it matches.

- Decryption: The decryption takes the cipher text *CT* as input and a secret key *SK* for an attributes set. It returns the message *Ms* if and only if it satisfies the access structure associated with the ciphertext *CT*. CP-ABFE depends on the attributes and policies which are associated with ciphertext, and the user decryption keys. The ciphertext is encrypted with an access tree policy that is selected by an encryptor and the corresponding decryption keys are generated with respect to the attribute set.

CP-ABFE will utilize the confidentiality preserving scheme to gain a fine-grained access control system. It consists of four preliminaries: CPA_Setup, CPA_Encrypt, CPA_KeyGen, and CPA_Decrypt.

i) CPA_Setup: Setup of CP-ABFE uses third party authority. Initially, G_1 consider as a bilinear group of prime order p, and g is a generator of G_1. Then select two random components α β Zp and establish public key and master key:

$$CPA_{PK} = \left\{ G_{1,g,h=g^{\beta}, f=g^{1/\beta}, e(g,g)^{\alpha}} \right\}, \quad CPA_{MSK=\{\beta, g^{\alpha}\}}, \tag{1}$$

ii) CPA_Fuzzy Encrypt: Sender makes the access policy T_M for the message about to be sent, encrypts plain text M , and gets ciphertext CT :

$$CT=CPA\_Fuzzy\ Encrypt(CPA_{PK}, M, A_T)$$

A submits two messages M_0, M_1 Î $G_{1,}$ if $M_0 = M_1$, B simply aborts and takes a random guess. The simulator flips a fair binary coin d, and returns the encryption of M_d. The Fuzzy encryption of FM_d can be done as follows:

$$C_0 = gc\ ,\ C\sim = FM_d\ e(g, g)\alpha c = FM_d\ Z \tag{2}$$

B generates, for wd, the ciphertext components {{ $C_{i,}$ t, 1, C_i, t, 2 } 1 ≤ i ≤ n_i } 1 ≤i ≤n as follows,

Set the root node of w to be c, mark all child nodes as un-assigned, and mark the root node assigned.

iii) CPA_KeyGen: The receiver submits its attributes set S to the authority and it uses CPA_{MSK} and S to compute the private key CPA_{pvk}, S:

$$CPA_PV_K, S = CPA\_Keygen\ (CPA_{MSK}, CPA_PV_K, S) \tag{3}$$

iv) CPA_Decrypt: In the end, receiver uses CPA_{pvk}, S to decrypt CT if S satisfies T_M , receiver will get M.

$$M=CPA\_Decrypt(CT, CPA_{pvk}, S, A_T) \tag{4}$$

Encryption time, key generation time and decryption time are calculated to evaluate the performance of CP-ABFE data outsourcing scheme.

7. Fuzzy Mathematical Model

Fuzzy logic is used for the decision that cannot be defined precisely. In such cases, the need of suitable knowledge representation for the notion makes the plausibility of fuzzy and which utilize problem-solving control system approach. The application of fuzzy deserves the following factors[11].

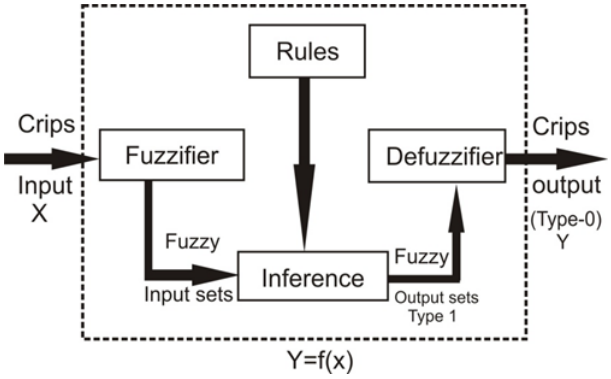

Figure 1. Fuzzy System.

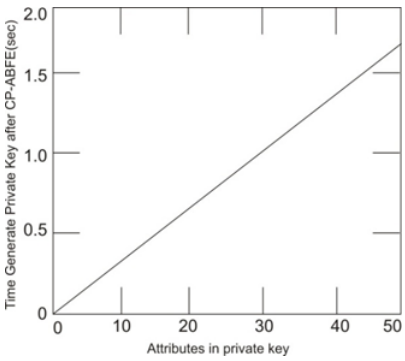

Figure 2. Key Generating Time.

- Conceptually fuzzy logic has greater understandability
- Mathematical concepts of fuzzy reasoning are simple[12].
- Fuzzy logic doesn't indulge with any far-reaching approach, it in an instinctive approach.
- It doesn't want to start with any scratches and flexi-

bility of the system and which comes out with more functionality. Even in case of careful looks, there is a chance of imprecise but fuzzy logic overcomes with these issues.

Fuzzy system can build to match any set of input data and used for nonlinear arbitrary functions. The fuzzy system does not replace the traditional control structure in turn it mixes together with the conservative control system. A Fuzzy System (FS) in Figure 1 consists of four main parts: fuzzier, rules, inference engine, and defuzzifier[13] .

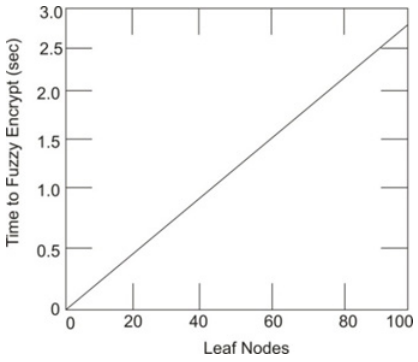

Figure 3. Fuzzy encryption time.

8. Fuzzy Algorithm

Steps

- Define the variables and terms (initialization)
- Construct the membership functions (initialization)
- Construct the rule specifications (initialization)
- Using the membership functions convert crisp input data to fuzzy values. (Fuzzification)
- Using rule base evaluate the rules (inference)
- Combine the results of each rule (inference)
- The output data should be converted to non-fuzzy values (defuzzification)

9. Function of FCSPS in CPA-ABFE

The developed model of Ciphertext-Policy Attribute Based Fuzzy Encryption allows a new type of encrypted access control where the user's private keys are denominated by a set of attributes. The encrypted data can state a policy over these attributes which specify the user ability for decryption[14]. Our system proposed a strategy of Fuzzy encrypted data that kept with confidentiality and secured against collusion attacks in a way it resists the collusion attackers from obtaining multiple private keys. The number of Cloud service providers has become popular in recent years and so the customer has a judicious option based on the parameters like cost, security, performance etc. The Fuzzy set A in X is denominated by a function $fA(x)$, which is related with each point in x in an interval of 0 and 1.

A fuzzy set can be defined mathematically by assigning its grade of membership to each probable individual in the universe. Hence these individuals of the fuzzy set may belong to the greater or lesser degree as per its membership function. The membership grades are frequently represented by using real number values which ranges within the closed interval of 0 and 1. The fuzzy sets are capable to express steady transition from membership to non membership and vice versa by using Fuzzy interface system.

10. Results

CP-ABFE-keygen runs in time precisely according to the number of attributes which associated with the issuing key. The running time of CP-ABFE is also almost entirely linear in access policy with respect to the leaf node counts. The polynomial notations of internal nodes quantify to a diffident number of multiplications and it doesn't contribute any significance to the running time. The experimental results show that the better search efficiency is achieved when the search input exactly matches with some predefined keyword, for the fixed value of d. The linear search technique is much more competent than the exiting approach in case of f = 1 and f = 2. The achieved results are used to validate our proposed model and identified that the solution is very efficient and effective in supporting fuzzy encrypted data search over Fuzzy CSP data.

11. Conclusion

In this work, we presented the construction of cipher text-policy attribute-based Fuzzy en-cryption data (CP-ABFE) to address the solution of security issues. In this system, a user's private key is associated with an arbitrary number of attributes which uttered as a string. On the other hand, if a party encrypts a message in our system, then that states an associated access construction over the attributes. It allows a user to decrypt a cipher text, if the user's attributes are passed through the cipher text access model.

12. References

1. Danan T, Chen S, Nepal S, Calvo RA. Secure data sharing in the cloud. Proc. Springer. 2013; 8(1):15–22.
2. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine grained access control of encrypted data. Proceeding of the 13th ACM Conference on Computer and Communications Security; 2006. p. 89–98.
3. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. Proceedings of IEEE Symposium on Security and Privacy; 2007. p. 321–4.
4. Lai J, Deng R, Guan C, Weng J. Attribute-based Encryption with Verifiable Outsourced Decryption. IEEE Transactions on Information Forensics and Security. 2013; 8(8):1343–54.
5. Zhu S, Gong G. Fuzzy authorization for cloud storage cloud computing. IEEE Transactions on Cloud Computing. 2014; 2(4):422–35.
6. Fu X. Cipher text policy attribute based encryption with immediate attribute revocation for fine-grained access control in cloud storage. IEEE International Conference on Communications, Circuits and Systems (ICCCAS); 2013. p. 103–8.
7. Zu L. New cipher text-Policy Attribute-Based Encryption with Efficient Revocation. IEEE International Conference on Computer and Information Technology; 2014. p. 281–7.
8. Xu Z. Dynamic user revocation and key refreshing for attribute-based encryption in cloud storage. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (Trustcom); Liverpool. 2012.
9. Li J. Fuzzy keyword search over encrypted data in cloud computing. IEEE Proceedings, INFOCOM; San Diego. 2010. p. 441–5.
10. Katherin VA, Alagarsamy K. A fuzzy mathematical model for performance testing in cloud computing using user defined parameters. International Journal of Software Engineering and Applications. 2013; 4(4):27–39.
11. Supriya M, Venkataramana LJ, Sangeeta K. Estimating trust value for cloud service providers using fuzzy logic. International Journal of Computer Applications. 2012; 48(19):28–34.
12. Ruj S, Stojmenovic M, Nayak A. Decentralized access control with anonymous authentication of data stored in clouds. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(2):384–94.
13. Koushik CS, Reddy KR, Reddy YR, Padmakumari P, Umamakeswari A. Location as attribute and re-encryption-based secure and scalable mechanism for mobile based applications in cloud. Indian Journal of Science and Technology. 2015; 8(12):65598.
14. Minutiae R, Ramachandran R. Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology. 2015; 8(S7):220–7.