ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

AVOIDING COMPUTATION OVERHEAD USING ABE SCHEME AND TRIVAL POLICY IN CLOUD

[1]Md Seraj Ahmad, [2]Dr.N.Srinivasan
Department of MCA (Prof. & Head of Faculty of Computer Science & Application), Sathyabama University, Chennai.
Email: mdseraj40@gmail.com

Received on 18-02-2016 Accepted on 20-03-2016

Abstract

CP-ABE (Cipher text-Policy Attribute-based Encryption) is regard as the major suitable method for access control of data in the cloud storage. In spite of obtainable Outsourced ABE resolutions able to delegate few intensive computing assignments to third party, verifiability results revisit from third party has as yet to address. The secure ABE Outsourced method is proposed to tackle above challenges. ABE (Attribute-based encryption) is standard encryption technique that permits users to decrypt and encrypt data based on attributes of user. It is conservatory attribute set encryption to develop flexibility and scalability at same time take over fine grained feature ABE access control. ABE encryption is flexible admittance control to encrypt and stored the data in cloud. It supports both decryption and outsourced key issuing security.

This method delegate every access policy and related attribute functions in decryption or key-issuing method to DSP (Decryption Service Provider) and KGSP (Key Generation Service Provider) leaving only simple process constant number for users eligible and attribute authority to complete locally. The ABE outsourced structure is proposed to provide check ability results of outsourced computation in efficient way.

Keywords: attribute based encryption, CP-ABE, DSP and KGSP.

1. Background

Internet tool is developing rapidly and people can store, process or share data. Cloud has materialized to provide different application services to convince of user's requirement. Cloud computing gives technologies and tools to construct information concentrated parallel applications by more reasonable prices compared to the traditional parallel

computing method. It has three different servicing models Platform as a Service (PaaS), Software-as-a-Service (Saas) and Infrastructure as a Service (IaaS).

Software-as-a-Service is kind of cloud computing permit the user to run previous online applications. Using multitenant architecture Saas delivers single application to more customers through browser. Using languages and specific tools platform as a Service permits the user to run users own applications. PaaS comprises environment for provisioning and developing cloud applications [1]. Infrastructure as a Service permits the user on a cloud to run any kind of application. IT resources are combined in IaaS linked to data storage resources, communications channel and computing resources. ABE gives secure way that permits the data owner to upload the data in untrusted storage as an alternative of trusted server. This advantage builds the methodology attractive in the cloud storage. In various organizations more number of user secure the access control in cloud. Moreover, key revocation, key management methods are necessary to scalable and secure ABE system [2].

In cloud storage service the data owner store the data in cloud and share the data to other users via cloud. For protecting stored data confidentiality need to encrypt before uploading in the cloud. The ABE encryption scheme to encrypt data it has two types CP-ABE (ciphertext-policy attribute-based encryption), KPABE (key-policy attribute-based encryption). Access policy allocated within private key in KP-ABE where CP-ABE specified ciphertext. The cloud computing development concerns data security. From public cloud sensitive data operated and maintained by CSP (Cloud Service Provider) [3].

In construction [4] initiated trivial policy by using AND gate organized by default attribute. Goyal et al. [5] explain identity based fuzzy encryption. Two various ABE complementary concepts were explained they are CP-ABE and KP-ABE [6]. Bethencourt et al. presented [7] generic group representation based on tree structure of CP-ABE construction. Access structures modes Concerning ABE revocation [8] delegatable revocation proposed to gain fine-grained and scalable control access.

To reduce local load distribute exclusive outside computational tasks [9]. To secure various modes expensive computations problem consider theoretical community of computer science. Atallah et al. proposed [10] a method for scientific computations secure outsource like quadrature and matrix multiplication. However, disguise technique leaded private information outpour. Li and Atallah investigated difficulty of computing two sequences distance [11].

2. Overall Architecture

Using check ability the outsource content we use four categories of service providers. Every service providers secures the content of user. AA (Attribute Authority), KGSP (Key Generation Service Provider), DSP (Decryption Service Provider), SSP (Storage Service Provider). Using ABE encryption technique Attribute Authority generate the key based on attributes of all user. The user set access control policy to particular file before uploading. For access policy user use their attributes also for a file set read/write control. Based on attributes of access control KGSP generates a key. After uploaded the file DSP provides the decryption key to every user. The SSP contain all encrypted keys and content. If a file uploading using service providers the content of file will securely outsource.

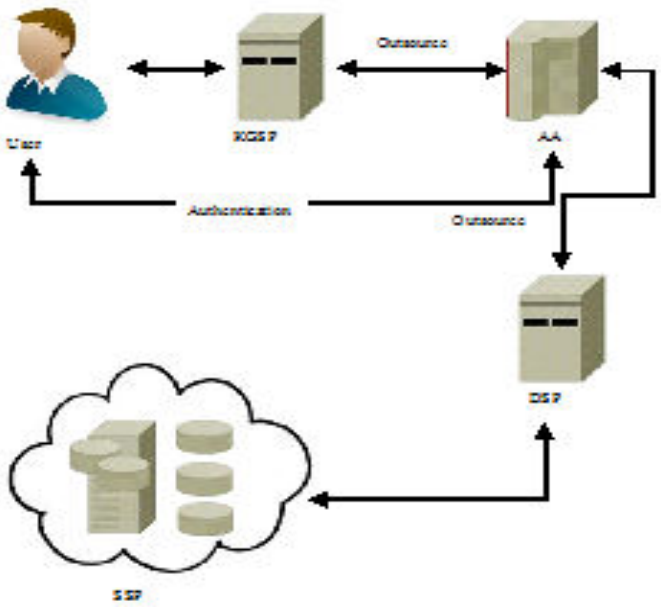

Figure-1: Cloud System.

3. Proposed System

3.1 Key Generation

By filling the personal details, user register their details. For authentication purpose user select the attributes based on these details. The KGSP and AA (Attribute Authority) is accountable to give authentication based on attribute of user by Elgammal algorithm. Using AES encryption technique performed the Key generation. AES encryption permit calculation performed on ciphertext. Through key generation AES randomly chooses two prime numbers. For every data while uploading the Secret key and Master key will generate to user authentication. Using AES technique key generated for encryption & decryption process.

3.2 User Authentication

In efficient ABE outsourcing method user authentication is a vital role. Through attribute authority perform user authentication while file uploading and KGSP perform while file downloading. Using Diffie Hellman algorithm user authentication is performed. For every file generate random key while uploading file. In user side, based on random value and attribute values performed using blind transformation. Blind transformation results on plaintext obtained by decryption. While downloading using KGSP perform authentication operation.

3.3 Data Storage and Retrieval

The system permits valid user towards upload file into SSP. The uploaded file encrypted and splitted so storage service provider can't able to get file. AES is used to encrypt file and split. Before encryption based on file type the file splitted after splitting operation convert into another file format. Splits have two servers so storage service providers can't able to obtain original file. If servers are negotiation then hackers get data. To get original data the user needs to extension file. The user obtain file after presenting file conversion, decryption and splits merging. Therefore it very secures in case of distrustful storage data service providers. Through file retrieval operation, KGSP is accountable to achieve authentication process.

3.4 Algorithm

Algorithm 1: EL-Gamal Digital Signature

Step1: Input (q, α, z); {α is S−smooth and divides q − 1, q ≅1 [4]}

Step 2: Input m; {d = h(D) where D is the data to be marked.}

Step 3: l ← (q − 3)/2;

Step 4: t ←α^{l} mod p; { t is the first constraint of digital signature and

have t := (q − 1)/α. }

Step 5: w ← (q − 1)/α;

Step 6: c ←α^{w} mod p; {c is a generator of a appropriate subgroup I}.

Step 7: S − z^{w} mod p; {S is an other element of I}.

Step 8: x0 ←x; { x is a explanation to the easy discrete logarithm difficulty c^{x} ≅B [p]}

Step 9: s $\leftarrow \frac{h(N)-txo}{l}$ [q − 1]; {s is the second constraint of digital signature. }

Step 10: Output (t, s). { Couple (t, s) is ElGamal digital signature devoid of by Alice private key x.}

Algorithm 2: Diffie Hellman

1. Two revelry are M and N. Both agree ahead two optimistic integers, n and g where g is group generator and n is prime number.
2. Revelry a randomly chooses optimistic integer x, smaller than n and it is called as M's private key. N also chooses private key y.
3. M and N calculate public keys by using A = ((g) ^ a) mod n and B = ((g) ^ b) mod n, respectively.
4. They swap public keys during communication channel.
5. Receiving keys, they will calculate shared key K, using K =(B) ^a mod n = (g) ^ab mod n and K = (A) ^b mod n = (g) ^ab mod n.
6. We examine a and b both are raised to originator which end to two exponentiations involved.

Algorithm 3: Data Encryption/Decryption Algorithm

DATA ENCRYPTION

Input: File Split

Output: File Encryption

1. Create symmetric key of AES using random value intended for every user.

2. Change file to byte array.

3. Using AES key encrypt byte array content.

4. Write encrypted data to file.

5. Store encrypted files to servers.

DATA DECRYPTION

Input: Key and Encrypted File

Output: Decrypted File

Step 1: Change file to byte array.

Step 2: Using AES key decrypt byte array content.

Step 3: Write decrypted data to file.

Step 4: Finally combines decrypted files.

4. Result and Discussion

4.1 User Registrations

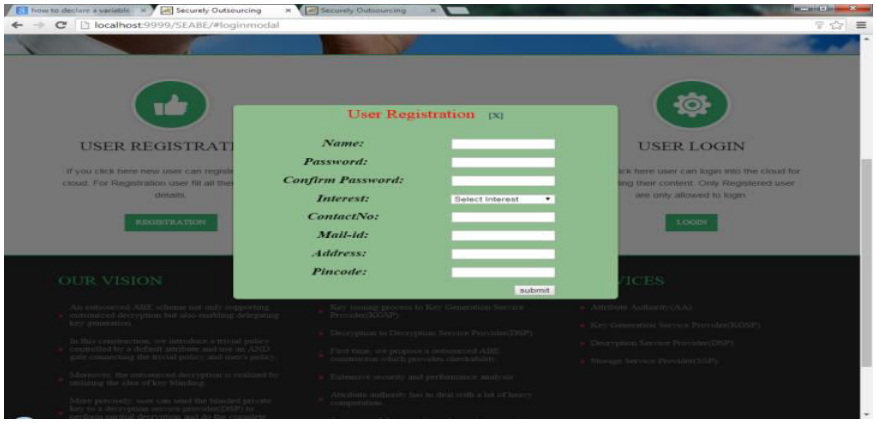

Figure-2: User Registrations.

In figure2 shows user registration. The users have to register their details in registration form in order to upload their file in cloud.

4.2 File Uploading

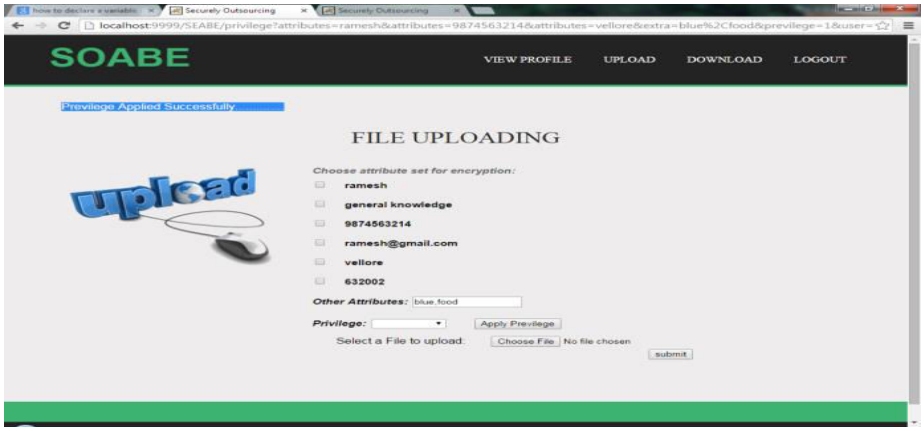

Figure-3: File Uploading.

In figure3 shows file uploading. The users have to choose file which they want to upload in to the cloud.

4.3 Key Generation Service Provider

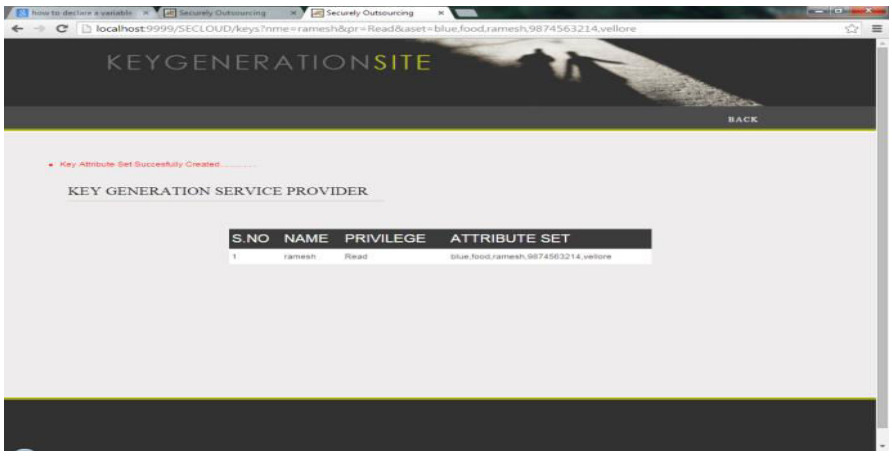

Figure-4: Key Generation Service Provider.

In figure4 shows key generation service provider. In key generation service provider generate the secret key and its shows the privilege and attribute set details.

5. Conclusion

ABE (Attribute-Based Encryption) is cryptographic basic which enormously enhances flexibility access control method. In ABE scheme, ciphertexts and private keys connected with access policies and attributes respectively. ABE efficient Outsourced system, maintains both decryption operations and secure outsource user authentication. This process offloads decryption or related attributes operation and access policy in information accumulating process to DSP (Decryption Service Provider) and KGSP (Key Generation Service Provider) authorization during data retrieval and AA (Attribute Authority) while data storing. The major advantage of this method highly secure when compare to ABE method also reduces overload attribute authority.

6. Reference

1. R.V.Agalya, K.Karthika Lekshmi, "A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 10, April 2014
2. Niloufer Rafath1, Wahaj Ghouri2, Syed Raziuddin," Security in Cloud using Ciphertext Policy Attribute-Based Encryption with Checkability", International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 3, Issue 5, May 2015
3. Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, „„Securely Outsourcing Attribute-Based Encryption with Checkability"", *Parallel and Distributed Systems,IEEE Transactions on,* On page(s): 2201 – 2210 Volume: 25, Issue: 8, August 2014
4. A. Sahai and B. Waters, „„Fuzzy Identity-Based Encryption,"" in Proc. Adv. Cryptol. EUROCRYPT, LNCS 3494, R. Cramer, Ed.,Berlin, Germany, 2005, pp. 457-473, Springer Verlag.
5. D.Boneh and M. Franklin. "Identity-Based Encryption from the Weil Pairing." Proc. Of CRYPTO"01, Santa Barbara, California, USA, 2001.
6. J. Bethencourt, A. Sahai, and B. Waters, „„Ciphertext-Policy Attribute-Based Encryption,"" in Proc. IEEE Symp. Security Privacy, May 2007, pp. 321-334.

7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, „„Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"" in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.
8. L. Cheung and C. Newport, „„Provably Secure Ciphertext Policy ABE,"" in Proc. 14th ACM Conf. CCS, 2007, pp. 456-465.
9. 10. M.J. Atallah, K. Pantazopoulos, J.R.Ricea,E.E. Spafford, „„Secure Outsourcing of ScientificComputations,"" in Trends in Software Engineering, vol.54, M.V.Zelkowitz,Ed.Amsterdam, The Netherlands: Elsevier, 2002, pp. 215-272.
10. S.Yu,C. Wang,K.Ren, and W. Lou, „„Achieving Secure, Scalable, Fine Grained Data Access Control in Cloud Computing,"" in Proc. IEEE 29th INFOCOM, 2010, pp.534-542.
11. M.J.Atallah and J.Li, Secure Outsourcing of Sequence Comparisons, "Int"l J.Inf.Security,vol. 4, no. 4, pp.277-287, Oct. 2005.

Corresponding Author:
Md Seraj Ahmad*,
Email: *mdseraj40@gmail.com*