VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SHARING DATA IN CLOUD BASED ON TRUST ATTRIBUTE BASED ENCRYPTION (TABE)

R. Manjusha[1] and R. Ramachandran[2]
[1]Department of Information Technology, Sathyabama University, Chennai, Tamilndu, India
[2]Sri Venkateshwara College of Engineering, Chennai, Tamilndu, India
E-Mail: manjushaphd14@gmail.com

ABSTRACT

Now a day's everyone storing there data in cloud because we can't depends on hard drives if they crash one can't have backup for ever data. Famous Cloud storage applications are Drop box, Google drive, Sky drive, Box, Amazon cloud drive, Surdoc and Apple icloud. In cloud data security is provided by various security algorithms. In our research we have chosen attribute based encryption technique to encrypt the data in cloud. We have proposed new attribute based encryption techniques which is known as trust attribute based encryption. In trust attribute based encryption first we find the trust of the attribute in web site and second based on trust attribute we from the access policy to cipher text. We propose scalable revocation scheme to trust based attribute based encryption by applying proxy re-encryption and lazy re-encryption to trust based attribute based encryption to provide efficiently revoke rights to users. We compare trust based attribute based encryption with key policy attribute based encryption; cipher text policy attribute and Hierarchical attribute based encryption based on time and number of attributes. We prove that trust based attribute based encryption is efficient compare to existing techniques.

Keywords: trust based attribute based encryption, proxy re encryption, lazy re-encryption, key policy attribute based encryption, cipher text policy attribute based encryption, Hierarchical attribute based encryption.

1. INTRODUCTION

Cloud computing is defined as sharing computing resources over internet. Different cloud computing layer available in market they are application service, application platform, server platform and storage platform. Application service provides software as a service examples are MS live\Exchange Labs, IBM, Quicken Online, Zoho and Cisco. Application Platform and server platform provides platform as services examples are Google App engine, Mosso,Force.com, Engine yard, Facebook, Heroku, AWS, 3Tera, EC2 and Linode. Storage Platform provides storage as service example is amazon s3 and dell. There are many encryption technique are available in cloud to encrypt the data. In our research we have chosen attribute based encryption technique to encrypt the data. The existing attribute based encryption techniques are Identity based encryption, key policy attribute based encryption; cipher text policy attribute and Hierarchical attribute based encryption based [1]. In identity based encryption public key is obtained from publicly known identity, private key is obtained from public key [2]. The example of identity based encryption is email address which is public key and password is private key. In key policy attribute based technique policies are associated with keys and attribute are associated with cipher text [3]. Cipher text attribute based encryption policies are associated with cipher text and\ - pttribute are associated with keys [4]. Hierarchical attribute based encryption is combination of hierarchical identity based encryption and cipher text policy attribute based encryption [5]. When data owner stores data in cloud server, user asks external audit party to maintain integrity of data. Without reading data content third party auditor should generate the audit report.

Security of sensitive data is maintained by using efficient Encryption scheme. To make security stronger we combine homomorphic encryption and attribute based encryption. We have proposed new attribute based encryption techniques which is known as trust based attribute based encryption. In trust based attribute based encryption first we find the trust of the attribute in web site and second based on trust attribute we from the access policy to cipher text. We propose a scalable revocation scheme to trust based attribute based encryption by applying proxy re-encryption and lazy re-encryption to trust based attribute based encryption to provide efficiently revoke rights to users. We compare trust based attribute based encryption with key policy attribute based encryption; cipher text policy attributes and Hierarchical attribute based encryption based on time and number of attributes. We prove that trust based attribute based encryption is efficient compare to existing techniques. In section3 we have discussed the architecture of trust based attribute based encryption. In section 4 we have discussed the implementation of trust based attribute based encryption. In section 5 we have discussed performance analysis of attribute based encryption. In section 6 conclusions of the paper is discussed.

2. ARCHITECTURE OF TRUST BASED ATTRIBUTE BASED ENCRYPTION

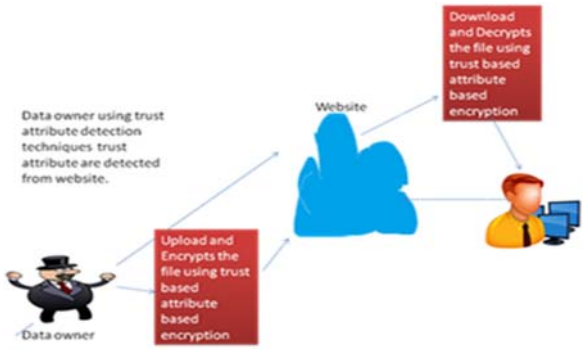

Figure-1. Architecture of trust based attribute based encryption.

In trust based attribute based encryption first we find the trust of the attribute in web site and second based on trust attribute we from the access policy to cipher text. Data owner find the trust attributes in websites using Trust attribute Detection Techniques then encrypts the file based on trust attributes uploads the file in cloud [3]. User decrypts the file from the cloud using trust attributes based decryption.

Implementation of trust based attribute based encryption

To implement trust based attribute based encryption we have consider hospital web site as example. From our observations in "home page", "contact us" and "privacy policy" pages trust attributes are present [6]. In a different format and different purpose the trust attributes are present in web site. We have built trustattribute of website based on ability, integrity and benevolence. Belief in skills of trusted party is known as ability. Belief in rules of conduct (honesty and keeping promises) of trusted party is known as integrity. Belief in making profit and wants to do good for the customer is known as benevolences. We have considered company website as example from that website we are finding trust attribute. Trust attributes are classified into three types Information based (IB), Function based (FB) and not classified (NC).Images and Text and images in website is classified as information based attribute. Data encryption and web site navigation is classified as Function based. Accuracy, competency, and competency are features of trust attributes which is classified as not classified. By taking online survey we can rank the 10 trust attributes. The survey is based on four steps they are 1) Setting up survey 2) Questionnaire design, 3) Survey implementation, 4) Data analysis. The trust attribute can found from user attribute table. Aftre calculation of trust and behavior data is passed inside attribute table which is dynamic in manner. We have proposed trust attribute based algorithm which has flowing steps

Step-1: In application server user can access the file after authentication.

Step-2: From user database we authorized user category and user attributes.

Step-3: Value of integrity of cloud service is obtained by verifying browserservice which is provided by cloud.

Step-4: Based on user activates on cloud trust of user is verified and trust values of user are calculated based on threshold and user policies.

Step-5: Based on historical data access of file trust of user is analyzed. The user can access the file based on access control policies and categorization.

Step-6: Data owner encrypts the file based on trust attribute based encryption. In this encryption is done by passing trust attribute as key. The key size is based on number of trust attributes used.

For example we have taken the hospital website as an example.

To find trust attribute in the websites we have taken a survey to user based on following question

Table-1. Question and option to user.

S. No.	Questions	Option to users
1	Infection control and sanitation	Good /Not Good/Bad
2	Medical record maintenance	Good /Not Good/Bad
3	Post master services	Good /Not Good/Bad
4	Nursing services	Good /Not Good/Bad
5	Satellite services	Good /Not Good/Bad
6	Pharmacy services	Good /Not Good/Bad
7	Physical plant maintenance	Good /Not Good/Bad
8	Quality assurance	Good /Not Good/Bad
9	Ambulance services	Good /Not Good/Bad
10	Social service	Good /Not Good/Bad

The Patient health data are controlled from one place to another in web. Health care records are stored in cloud server and encrypted using trust based attribute based encryption. User can decrypt the data if and only if he satisfies the Trustbased access policy.

User Revocation based on Trust based attribute based Encryption.

Data owner has to re-encrypt the file user has to access which leads to computation overhead. The solution to this problem is two layered trust based encryption and Proxy Trust Re-Encryption. In two layered trusts based encryption data owner encrypt data based on trust based encryption and again cloud encrypts data based on trust based encryption. In proxy trust encryption third party encrypts the data which is already encrypted using homomorphic encryption .Homomorphic encryption is a encryption in cipher text computation is performed which

generates encrypted results when decrypted matches the results of plaintext [7].

3. PERFORMANCE ANALYSIS OF ATTRIBUTE BASED ENCRYPTION

The performance of trust based attribute based encryption is based number of attribute and time taken to encrypt and decrypt the file. The execution time of trust based attribute encryption is less compare cipher text attributes based encryption and key policy attributes based encryption [8]. Security of Trust based attribute based encryption is high compare to cipher text attributes based encryption and key policy attributes based encryption because encryption is based on trust attributes [9]. The data owner can create and define new access policy based on behavior of user and history of the user. Fine gained access control is achieved depending on access policy [10]. User access privileges and confidentiality is achieved by trust based attribute based encryption. User secret key accountably achieved by trust based attribute based encryption protect the key abusers. Data confidently is achieved through trust based attribute based encryption [11].

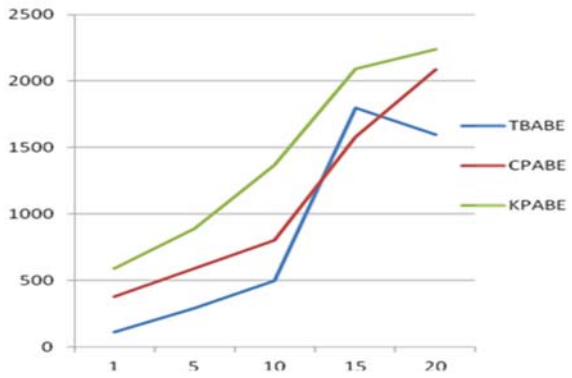

Figure-2. Number of attributes Vs execution in ms.

4. CONCLUSIONS

Security of Trust based attribute based encryption is high compare to cipher text attributes based encryption and key policy attributes based encryption because encryption is based on trust attributes. Fine gained access control is achieved depending on access policy. User access privileges and confidentiality is achieved by trust based attribute based encryption. User secret key accountably achieved by trust based attribute based encryption protect the key abusers. Execution time of trust based attribute based encryption is less compare to cipher text attributes based encryption and key policy attributes based encryption. Data confidently is achieved through trust based attribute based encryption. Trust based attribute revocation is fast compare to other attribute based encryption techniques.

REFERENCES

[1] Guojun Wanga, Qin Liu, Jie Wub, Minyi Guo," Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", computers and security 30 (2 011) 320-3 3 1.

[2] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proc. of EUROCRYPT 2004, volume 3027, LNCS, 54-73. Springer.

[3] R. Manjusha, R. Ramachandran, "Web mining framework for security in e-commerce", Recent Trends in Information Technology (ICRTIT), 2011 International Conference,ISBN:978-1-4577-05885.

[4] Page(s):1043-1048, Publisher: IEEE, Date of Conference: 3-5 June 2011.

[5] R. Manjusha, R. Ramachandran," Comparative study of attribute based encryption techniques in cloud computing", Embedded Systems (ICES), 2014 International Conference on Embedded Systems, Print ISBN:978-1-4799-5025-6, Publisher IEEE, 3-4, July 2014.

[6] J. Jospin Jeya, E. Kannan,"Multi Key Word Search and Trusted Auditing System to Verify the Integrity of Outsourced Data in Cloud Computing", International Review on Computer and Software (IRECOS), 2014, vol. 9, No. 10, pp. 1962-1964.

[7] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol, Information Sciences", 2011, 181(19): 4318-4329.

[8] R.Manjusha, R.Ramachandran," Highly Secured Cloud Computing using Functional Encryption Scheme", Information journal, japan, vol.17, no. 9(b), September, 2014.

[9] Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan Nickolai Zeldovich,"Reusable Garbled Circuits and Succinct Functional Encryption", STOC'13, June 1-4, 2013, Palo Alto, California, USA. Copyright 2013 ACM 978-1-4503-2029-0/13/06 ...$15.00.

[10] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J.,Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited:

Consistency properties, relation to anonymous IBE, and extensions. J. Cryptology 21(3), 350-391, 2008.

[11] Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: Functional encryption for inner product Predicates from learning with errors. Cryptology ePrint Report 2011/410 (2011), http://eprint.iacr.org.

[12] D. S. Shaji, E. Baburaj,"Green Cloud: An Energy Efficient Load Balancing Approach Using Global Load Optimization", International Review on Computer and Software (IRECOS,), Vol 9, No. 8 2014, pp.1408-1416.