Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.142 – 146

A Review on Attribute Based Encryption (ABE) and ABE Types

Ashwini K.M[1], Umashankar B.S[2]
[1] 4th SEM, M.Tech, Dept. Of Computer Science & Engg, Adyar, Mangaluru, India
[2] Professor, Dept. Of Computer Science & Engg, Adyar, Mangaluru, India
[1] ashwini.km21@gmail.com; [2] umashankar.cs@sahyadri.edu.in

Abstract— now a day's in the latest computer environment data are shared and stored on the Internet. To maintain huge amount of information's in the cloud storage done through internet, for this latest growing technology is used called as Cloud computing. Privacy and security must be must be provide for the information. For giving privacy for the data Attribute Based Encryption plays a role in the trusted cloud platform. ABE is one kind of public key encryption. In which the ciphertext is dependent on the private key. While decrypting the message the attribute of the cipher text should match with group of attributes of the client's key. Here we also discussed about two types of ABE methods. They are KP-ABE and CP-ABE. The comparison works of two methods are done in this paper

Keywords— Attribute based encryption, privacy, security, cloud storage, KP-ABE, CP-ABE

I. INTRODUCTION

In the modern world huge amount of data's are generating rapidly. To store these data cloud storage is used which is accessed through internet. The user should have the knowledge of data leakage and unauthorized access of data, because the cloud works on "pay and use" policy [1]. A cloud is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service) [6].

The user should take care about of accessing data. The user should have flexible and scalable data access policies for his information. He can give the accessing of data only for an authorized user. The main concept of cloud is it should give privacy, security, confidentiality and safe access control to the information stored in the cloud.[5] To help the user an Encryption of data came into picture to give the privacy and security for the data. Only authorized users could get the decryption key. But in this some problem are occurred. When numbers of authorized users are increased at that time it creates problem in scalability, flexibility and it is not efficient. To overcome from this problem an Attribute Based Encryption Algorithm was introduced [2].

In this paper we concentrated on review work of Attribute based encryption. Section II deals with literature work on various encryption methods. Section III concludes the discussions.

© 2016, IJCSMC All Rights Reserved

II. LITERATURE SURVEY

To store the data in the cloud we need security and privacy. For safe storing and sharing of the data the user must store the data in the form of encryption. Encryption was help to avoid the unauthorized access of data from the cloud[4]. To give the security, privacy and confidentiality for the data stored in the cloud various methods are introduced. One of the encryption techniques is Attribute based encryption technique which is used to give the privacy, security, confidentiality and safe access control for the data.

The ABE algorithms having two types; one is Key Policy ABE (KP-ABE) and another one Cipher Policy ABE (CP-ABE). In the KP-ABE, the attribute policy and data are connected to keys and attribute respectively. In CP-ABE, the attribute policy and data are connected to attribute and keys respectively.

A. *Attribute Based Encryption **(ABE)***

The Attribute Based Encryption (ABE) algorithm is one kind of public key encryption. In Older encryption method by using user's public key all the data's are encrypted, that key is sharing with many people. Because of this reason existing encryption method is incompetent[3]. In ABE method Key Authority came into picture. Generating the keys for the encrypting and decrypting a message is a major role for Key Authority. KA generates the keys based on users attributes. If the user wants to add some attributes or remove some attributes then KA collect the new attributes and generate new public and private key based on new attributes[4]. In ABE the message is encrypting using user's public key and receiver will decrypt the message using private key which is sent by Key Authority.

B. *Key Policy Attribute Based Encryption (KP-ABE)*

Key Policy (ABE KP-ABE) is a customized form of ABE. This method is mainly used for one-to-many communication. In the KP-ABE the encrypted data are connected with set of attributes and secret key are labeled with access tree structure. The data sharing is the main application of KP-ABE in the un-trusted cloud storage[7]. The combination of Re-encryption and KP-ABE method gives the efficient result for user revocation in the cloud platform, this helps to good access control. In cloud server the KP-ABE method helps to lessen the majority of computational transparency (overhead). A fine grained access control is provided by the KP-ABE encryption scheme. In this scheme data is firstly encrypted using the symmetric data encryption key then again re-encrypting that data using public key consequent to set of attributes [8]. The key authority is decides who can decrypt the data. KP-ABE is not suitable for certain application.

C. *Cipher Policy Attribute Based Encryption (CP-ABE***)**

CP-ABE is one form of Identity Based Encryption. In this one public key and one single master key. By using that single master key different restricted private keys are generating corresponding to set of attributes. CP-ABE depended by cipher text and users which are interconnected with attributes and policy. The data is encrypting using access policy and same message decrypting using attributes[10]. A client ought to just be proficient to get to the information in a few scattered frameworks if a client complies with a guaranteed set of capabilities or trademark. In this a present technique was compelling to obey such standards to take up a trusted server to store the information and referee affirmation control. The security of information will be traded off if any server putting away the information is bargained. Here a framework is introduced to know the multifaceted nature of permission control of encoded information called as Ciphertext-Policy Attribute-Based Encryption. Contrasted with before ABE this technique giving better execution[12]. In this work creator specified around a framework trademark that is utilized to clarify a client's accreditations and approach for decoding of information. This technique was best for impact strike[16]. We can keep information more secure in the un-trusted server utilizing this method.

III. RESULTS

In this paper we compared two types of ABE technique with different parameters, shown in below Table I. The ABE gives a strapping groundwork for encryption scheme and access control. Here we discussed two type of ABE, i.e. KP-ABE and CP-ABE. One of the main advantages of CP-ABE is that by deciding who can decrypt the data which was stored in cloud.

© 2016, IJCSMC All Rights Reserved

TABLE I
COMPARISON OF ABE METHODS

Algorithm [13,14]	Features					
	Computation Overhead	Decryption and User revocation Efficiency	Collusion resistant	Application Relevancy	Association of Attributes	Association of Access Policy
ABE	Average	Average	Below Average	Supports users with similar attributes	With Ciphertext	With Key
KP-ABE	High	Low	Average	Supports users with dissimilar attributes based on key policy	With Ciphertext	With Key
CP-ABE	High	Low	Yes	maintain users with different attributes structured in single set	With Key	With Ciphertext

Table II, showing the comparison between KP-ABE and CP-ABE techniques. The access control feature is low in KP-ABE compared to CP-ABE. But when KP-ABE is connected with re-encryption scheme then it gives the high access control for data. In KP-ABE efficiency is more when it connected with broadcast type encryption. CP-ABE is gives best result compared to KP-ABE, which is not suitable for modern atmosphere

TABLE III
COMPARISON OF KP-ABE AND CP-ABE

Parameters/ Techniques	**KP-ABE**	**CP-ABE**
Access Control [11,15]	Low High if connected with re-encryption technique	Average understanding of complex access control
Efficiency	Average High for broadcast type encryption	Average Not efficient for modern enterprise environment

The Fig1 shows below the comparison graph. It compares three kinds of algorithm with respect to Computational overhead.

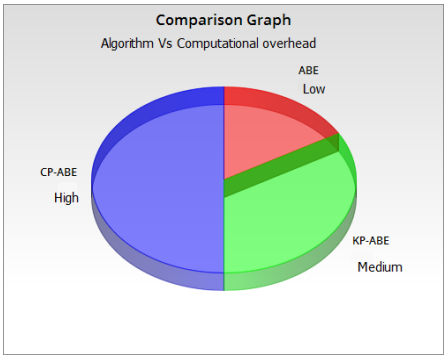

Fig. 1 Comparison Graph

The Fig.2 shows the graphical representation of types of ABE algorithm with respect to execution time vs. number of attributes. Graphs are showing the average overhead timing for both KP-ABE and CP-ABE algorithm[17].

© 2016, IJCSMC All Rights Reserved

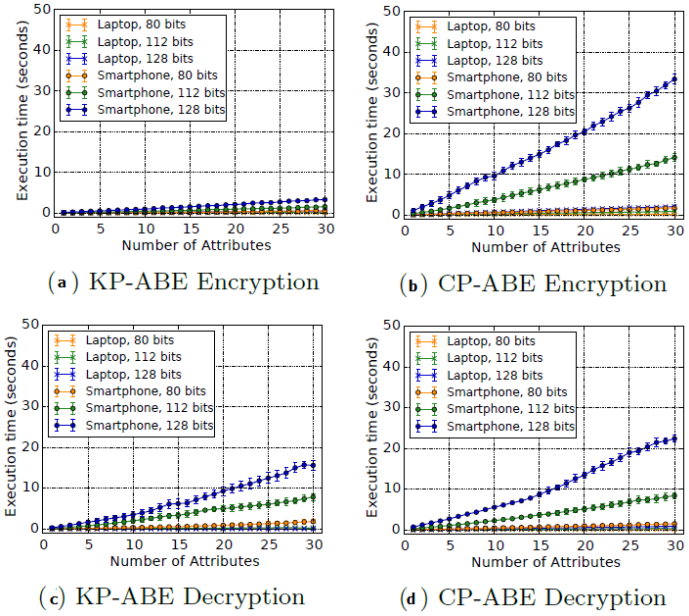

Fig 2. Average Execution Time

IV. CONCLUSIONS

In this paper, we discussed about ABE technique and its two types. The ABE method is mainly used for access control. This helps to filter the user for accessing data. Key strength is the main advantage of ABE, which helps a make a strong encryption compared to old encryption. Here we compared the ABE techniques and its two types with different features. Every method is better than other methods. This gives the best security and privacy for each data in the cloud. Also provide fine access control and efficiency.

REFERENCES

[1] Cloud Computing by wikipidia ,https://en.wikipedia.org/wiki/Cloud_computing.
[2] Baodong Qin, Robert H.Deng, Shengli Lu,Siqi Ma: Attribute Based Encryption with Efficient Verifiable outsourced Decryption. IEEE Transaction on Information Forencsics and security. Vol. 7,pp: 1384—1393(2015).
[3] Attribute Based Encryption. Wikipedia(https://en.wikipedia.org/wiki/Attribute-based_encryption).
[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010
[5] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.
[6] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52
[7] Chang-ji Wang,Jian Fa Luo: A Key-policy Attribute-based Encryption scheme with Constant size Ciphertext. Eight International Conferences on CIS. Guangzhu (2012)
[8] Changji Wang,Yang Liu: A secure and Efficient Key-Policy Attribute Based Key Encryption Scheme. International conference on Information science and Engineering, pp. 1601—1604, Nanjing(2009).
[9] Junbeom Hur.:Improving security and Efficiency in Attribute-Based Data sharing.IEEE transaction on Knowledge and data engineering.(2013).
[10] John Bethencourt., Amit Sahai., Brent Waters.: A Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy.Barkeley,CA (2007).
[11] Jin Li,. Gansen Zhao,.Xiaofeng Chen,.Dongqing Xie,.Wenjun Li,. Lianzhang Tang,. Yong Tang.:Fine-grained Data Access Control Systems with User Accountability in Cloud Computing. In. 2nd conference cloud computing technology and science, pp: 89-96. Indianapolis, IN (2010).
[12] Longhui Zu,.Zhenhua Liu,.Juanjuan Li.:New Ciphertext-Policy Attribute-Based Encryption with Efficient Revocation. International Conference on Computer and Information Technology (2014).
[13] Balamurugan B, Venkata Krishna P: Extensive Survey on Usage of Attribute Based Encryption in cloud. Journal of Emerging Technologies in web Intelligence. vol. 6 , (2014).
[14] Minu Geroge, C.Suresh Gnanadhas, Saranya. K: A survey on Attribute Based Encryption Scheme in Cloud Computing. IJARCCE, vol. 2(2013).

© 2016, IJCSMC All Rights Reserved

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE INFOCOM'10*, 2010
[16] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009
[17] Moreno Ambrosin, Mauro Conti, Tooska Dargahi: On the Feasibility of attribute –based encryption on Smartphone devices. IoT –Sys. ACM, Florence, Italy(2015)

© 2016, IJCSMC All Rights Reserved