Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Attribute Based Cryptographically secure (ABCs) Encryption In Cloud Computing: Analysis and Comparative Study

Rahul Vora[1], Prof. Priyanka Raval[2], Prof. Kunjal Garala[3]

[1]*Computer Engineering, B. H. Gardi College of Engineering & Technology*
[2]*Computer Engineering, B. H. Gardi College of Engineering & Technology*
[3]*Information & Technology, B.H Gardi College of Engineering & Technology*

Abstract — In today's digital world Cloud computing is a revolution knowledge for stream of computing as a utility. That is providing platform and services for enormous-scale of data storage and data manage. Big Data on cloud environment analyze, storage, manage, visualization, security are some challenges that requires more timing and large computation infrastructure processing. Security in terms of data Protection is one of the challenges that overcome use of cryptographic framework through access control mechanism. In this paper we discussed, compared and analyzed of Attribute Based Cryptographically secure (ABCs) Encryption algorithm.

Keywords-Cloud Computing; Literature Survey; Comparative study; Cryptographic; ABE

I. OUTLINE

Cloud or distributed Computing is an innovation. It is not invention or discovery that is new building of old elements producing a new collaboration. It is the provision of computing facilities over the Internet that permit to use software and hardware that are manage at remote locations by third parties. Cloud service resources mainly lying on two aspects that (a) "Access anywhere and anytime" and (b) "Pay-as-you-go.

Recently Cloud Computing has become one of the popular techniques used by both industry and educational institutions in order to provide flexible way to store and access the data files. Cloud Computing can be defined as "structural model that defines computing services where resources as well as data are retrieved from cloud service provider via Internet through some well-formed web-based tools and application."

The further of this paper is structured as: Section II presents Contextual of ABE. Section III delivers Literature Survey. Section IV presents construction of ABE scheme and cp-abe toolkit and Section V shows the conclusion and future work.

II. CONTEXTUAL OF ABE

The term encryption mentions to converting the original data into human illegible form and reverse is known as decryption. The data encrypting only the authorized person can decode to achieve confidentiality. The attribute based cryptographically secure encryption is verified algorithm for cloud computing environment.

In ABE scheme, attribute plays significant role. It generally includes encrypting the attributes neither encrypting the entire data. Attributes have been exploited to generate a public key for encryption data and have been used as an access policy to control users' access [1]. Based on the access policy, subsequent researches can be roughly categorized as either key-policy or ciphertext-policy. The fig 1 represents the taxonomy of different types of ABE.

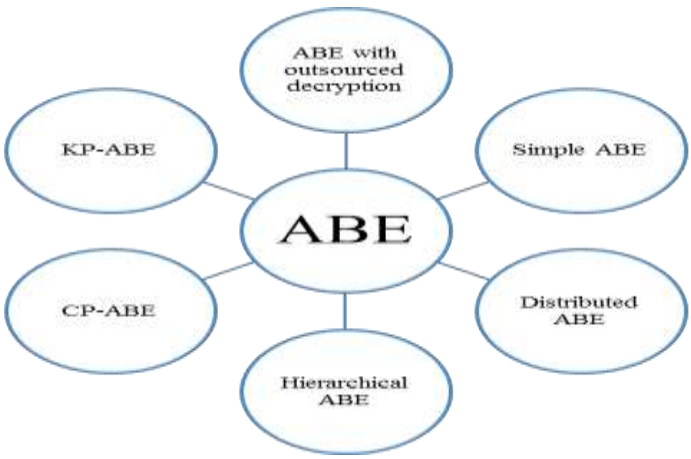

Figure 1. Taxonomy of ABE

The first KP-ABE scheme that allows any monotone access structures was proposed by Goyal et al. [2], and the first CP-ABE scheme was presented by Bethencourt et al. [3]. After that, several antiquity of ABE schemes were proposed as shown in figure 2.

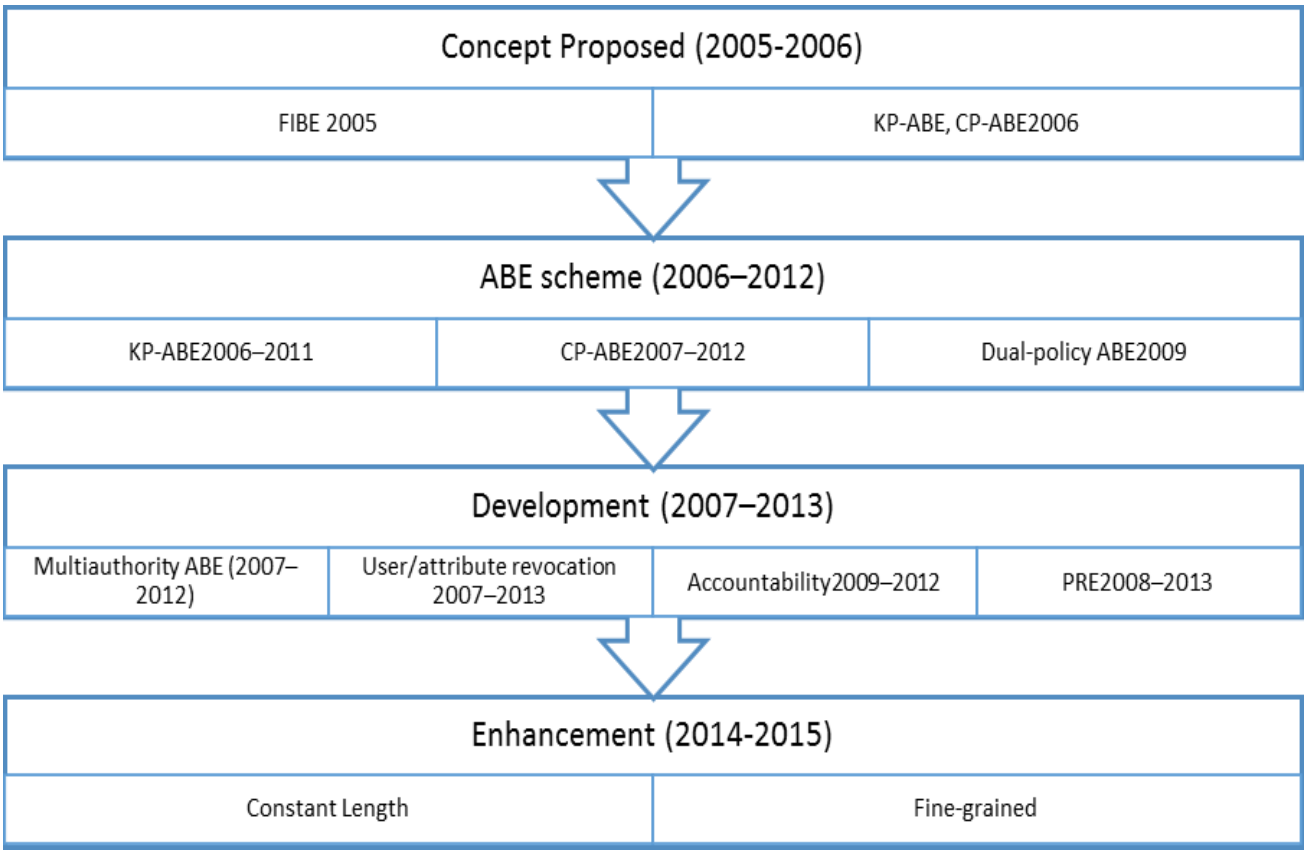

Figure 2. Antiquity of ABE

KP-ABE: Key-Policy Attribute Based Encryption
CP-ABE: Ciphertext-Policy Attribute Based Encryption
FIBE : Fuzzy Identity Based Encryption
PRE : Proxy Re-Encryption
CL : Constant –Length

The cryptographic secure access control ensures that ABE technique is widely used in the Cloud Computing. Two main ABE schemes exist in the literature, namely: The Key Policy Attribute Based Encryption (KP-ABE) scheme and the Cipher-text Policy Attribute Based Encryption (CP-ABE) scheme as shown below:

2.1 KP-ABE

The Key-Policy Attribute Based Encryption (KP-ABE) is an ABE scheme where the access structure is embedded in the users' private keys, while the cipher-texts are labeled with attributes [4]. A user is able to decrypt a cipher-text if the latter attributes satisfy the access structure of the key [4]. Figure 3 shows the scheme of KP-ABE.

2.2 CP-ABE

The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) differs from KP-ABE in that the keys are used to describe the users' attributes and the policy defining who is able to decrypt data is embedded in the ciphertext [4]. Figure 4 shows the scheme of CP-ABE.

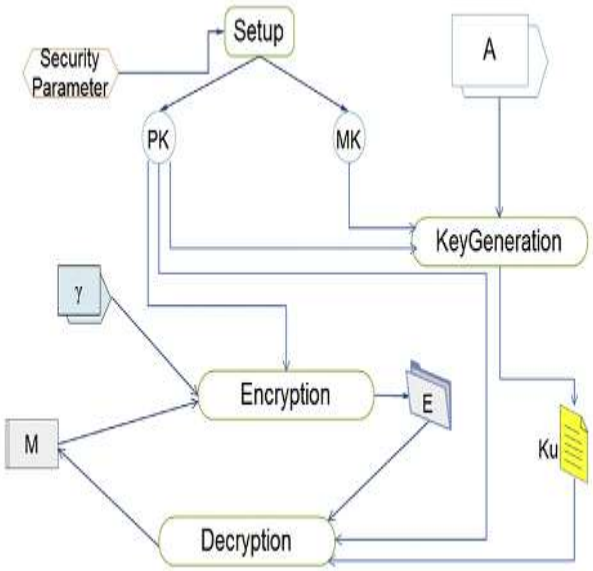

Figure 3. Scheme of KP- ABE [4]

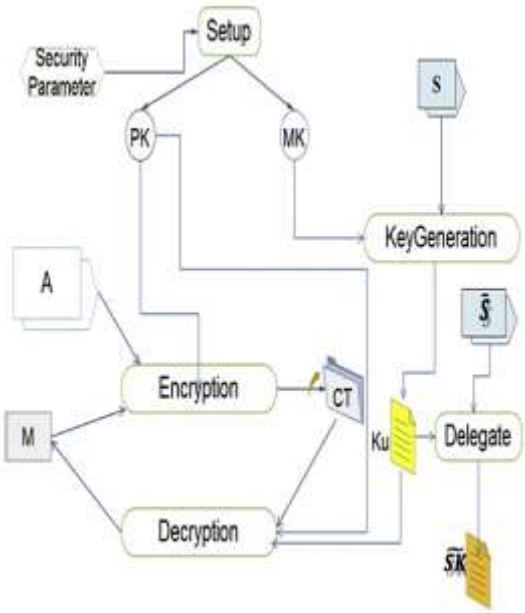

Figure 4. Scheme of CP-ABE [4]

III. LITERATURE SURVEY

Balamurugan et al. [6] discussed revenue of cloud computing as well as importance of encryption method in cloud critical application or server. Also described features of Attribute Based Encryption (ABE) such as delivers flexible access control with the help of different key management approaches, low-cost, easy and secure from others encryption techniques. Also described classification of cloud based High, Medium and low critical applications through different attributes such as timeliness, accuracy, security, privacy, etc. Also showed critical application chart that based on risk. They proposed simplified based ABE algorithm with the help of digital signature, private key, public key, hash function mapping, access structures and secret key functionalities. Also in that proposed algorithm 3 level security with dual authentication and secret key- private key matching concepts using hash function was there so quite difficult to hack it, so, if all 3 level was successfully executed then and then decrypt the original data and secure for user as well as CSP point of view.

Tebibel et al. [4] proposed to improve confidentiality of outsourced data and when search was performed over encrypted data, emphasizing access control on search result with the help of ACAS (Access Control Aware Search) principle for personalized or multi user accessing data. Due to limits as Extra filer authority on the user side, trust mechanisms as well as maintenance and highly searching time were found in Kaci et al. (2014) proposed method, they proposed xSE-ACAS for reducing time, parallelization, multi keyword search and showed the advantages behind the used of two access control techniques performance. xSE-ABE model designed for ensuring access control on the result of searchable encryption to integrate SSE with ABE (CP-ABE) access policy. xSE-ACAS model designed for securing data outsourced to the cloud that known to be “honest-but-curious”. Because search services behaves honestly but catch some confidential information of users. Also, that consider as multi keywords search and sequential search.

Horvath et al. [7] made ABE more effective for access control to storing data in the cloud and focused on access rights, key management, user revocation and different authorities. System was made feasible by removing or computational overhead from CSP or distributed over large number of users. To avoiding re-encryption of all cipher texts that access structure contain subset of attributes of the revoked user, proposed scheme that adds ID based user revocation feature to distributed CP-ABE for security and efficiency.

Here we study the no of research paper and then make the Literature survey table and comparative study table for the different techniques in ABE.

Ref no	Paper Title	Description & Methods	Input Parameters	Observed Technique
[4]	Parallel search over encrypted data under ABE on the Cloud	To improve confidentiality of outsourced data and proposed xSE-ACAS for multi keyword searching and xSE-ABE model	symmetric key K, Build Index I	"honest-but-curious" –search services
[5]	Fine-Grained Access Control for Big Data Based on CP-ABE in Cloud Computing	To proposed novel access control policy based on CP-ABE to achieve fine-grandees and effectively implemented operation of user revocation	PK, MK, M, SSK, New file creation, New User Grant, User Revocation	AND, Or, Not, Threshold, Preventing Collusion, Data Confidentiality
[6]	Enhanced Attribute Based Encryption for Cloud Computing.	To proposed simplified based ABE algorithm with the help of digital signature, private key, public key, hash function mapping, access structures and secret key functionalities.	PK, SK, Hash function H(x), Digital Signature	Dual Authentication
[7]	Attribute-Based Encryption Optimized for Cloud Computing	More effective for access control to storing data in the cloud & focused on access rights, key management, user revocation and different authorities.	Linear Secret Sharing Schemes (LSSS), Global Setup(λ), Central Authority Setup(GP)	prevent collusion attacks, identity-based user revocation in multiauth. CP-ABE
[8]	A Novel approach for searchable CP-ABE with hidden Ciphertext-policy	To Proposed to new searchable CP-ABE scheme that allows the authorized user to check whether the ciphertext contains specific set of keywords or not Test multiple keywords searching and collusion resistant	Discrete Logarithm Problem - a ∈ Zp, DBDH assumption, Access structure, GenToken(MSK,K), Encrypt_KS(MPK, CT, KW):	AND gate with negative attributes and wildcard
[9]	Self-contained Data Protection Scheme Based on CP-ABE	They proposed to Extended CP-ABE (ECP-ABE) schemes that express any ABAC policies represented by arithmetic comparison and added some extra logical expression as NOT, <,>	PK, MK, M, exp(N.O.V), i.e. "attribute name operator attribute value"	AND,OR,NOT,<,≤,>,≥, [ ],( ), ( ] and [ ) operators

Table 1. Literature Survey

Parameter Ref. Papers	Basic Idea (BDCC)	Confidentiality	Security	Efficiency	Comp. Over head	Revocation	Flexibility	Mul. Auth.	searching
[1]	Y	-	-	-	-	-	-	-	-
[4]	-	Y	-	-	-	-	-	-	Y
[5]	-	-	-	-	Y	Y	-	-	-
[6]	-	-	Y	-	-	-	-	-	-
[7]	-	Y	-	-	-	Y	Y	-	-
[8]	-	-	Y	Y	-	-	-	-	Y
[9]	-	-	-	Y	-	-	-	-	-
[10]	-	-	-	Y	-	-	-	-	-
[11]	-	-	Y	Y	-	-	-	-	-
[12]	-	-	Y	-	-	-	-	Y	-
[13]	-	-	Y	Y	-	-	-	-	-
[14]	-	-	Y	-	-	-	-	-	-

Table 2. Comparative Study

IV. CONSTRUCTION OF ABE SCHEME

4.1 Preliminaries

4.1.1 Bilinear Maps: Let G1,G2,GT be cyclic (multiplicative) groups of order p, where p is a prime. Let g1 be a generator of G1, and g2 be a generator of G2. Then e :G1 × G2 ! GT is a bilinear map if it has the following properties:

1. Bilinearity: for all u 2 G1, v 2 G2 and a, b 2 Zp, we have e(ua, vb) = e(u, v)ab.
2. Non-degeneracy: e(g, h) != 1.Usually, G1 = G2 = G. G is called a bilinear group if the group operation and the bilinear map e are both efficiently computable.

4.1.2 Access Structure: Let {P1, P2, . . . , Pn} be a set of parties. A collection A ⊆ 2{P1,P2,...,Pn} is monotone if ∀B,C : if B ∈ A and B ⊆ C then C ∈ A. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {P1, P2, . . . , Pn}, i.e., A ⊆ 2{P1,P2,...,Pn}\{∅}. The sets in A are called the authorized sets, and the sets in A are called the unauthorized sets.

4.1.3 Fundamental Algorithm: An ciphertext-policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, KeyGen, and Decrypt. In addition, we allow for the option of a fifth algorithm Delegate.

- **Setup (PK,MK)** The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.
- **Encrypt (PK,M,A)**. The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.
- **Key Generation (MK,S).** The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.
- **Decrypt(PK,CT,SK).** The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.
- **Delegate(SK, ˜ S).** The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S˜ ⊆ S. It output a secret key S˜K for the set of attributes ˜ S.

4.2 Simulation Tool

To Modified CP-ABE scheme and after that algorithm testing purpose, below tool required for the simulation as :

- **Cpabe toolkit –** For install this tool firstly we required below 3 packages as:
  1. **Gmp library**
  2. **Pbc (Pairing based cryptography) library**
  3. **Libbswabe**

V. CONCLUSION AND FUTURE WORK

On the basis of Analysis, Literature reviews, survey and working simulation process conclude that regarding security in cloud environment still need to be some appropriate changes with help of CP-ABE parameter and access mechanism. Also improving data protection and decrease computational overhead and complexity.

Future Work:

- ✓ Use BYOK concept for addition security.

REFERENCES

[1] L. PANG, J. YANG, AND Z. JIANG, "A SURVEY OF RESEARCH PROGRESS AND DEVELOPMENT TENDENCY OF ATTRIBUTE-BASED ENCRYPTION.," SCI. WORLD J., VOL. 2014, P. 13, 2014.

[2] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Comput. Commun. Secur., pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," Proc. - IEEE Symp. Secur. Priv., pp. 321–334, 2007.

[4] T. Bouabana-Tebibel and A. Kaci, "Parallel search over encrypted data under attribute based encryption on the Cloud Computing," Comput. Secur., vol. 54, pp. 77–91, 2015.
[5]] Q. Yuan, C. Ma, and J. Lin, "Fine-Grained Access Control for Big Data Based on CP-ABE in Cloud Computing," pp. 344–352, 2015.
[6] N. Systems, "Attribute-Based Encryption Optimized for Cloud Computing," pp. 566–577, 2015.
[7] P. Pääkkönen and D. Pakkala, "Big Data Research Reference Architecture and Classification of Technologies, Products and Services for Big Data Systems", Big Data Res., vol. 1, pp. 1–21 (2015)
[8] M. Padhya and D. Jinwala, "A Novel Approach for Searchable CP-ABE with Hidden Ciphertext-Policy," pp. 167–184, 2014.
[9] M. Kandias, L. Mitrou, V. Stavrou, and D. Gritzalis, "E-Business and Telecommunications," Commun. Comput. Inf. Sci., vol. 456, pp. 270–289, 2014.
[10] N. Rafath, W. Ghouri, and S. Raziuddin, "Security in Cloud using Ciphertext Policy Attribute-Based Encryption with Checkability," pp. 4427–4434, 2015.
[11] S. Yakoubov, V. Gadepally, N. Schear, E. Shen, and A. Yerukhimovich, "A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud," 2014.
[12] R. Manjusha, "Comparative Study of Attribute Based Encryption Techniques in Cloud Computing," no. Ices, pp. 116–120, 2014.
[13] P. Rajput, "Highly Secure Method based on Ciphertext Policy Attribute based Encryption in Hadoop System," vol. 103, no. 9, pp. 34–38, 2014.
[14] N. Doshi and D. Jinwala, "Hidden Access Structure Ciphertext Policy Attribute Based Encryption with Constant Length Ciphertext," Adv. Comput. Netw. Secur., vol. 7135, pp. 515–523, 2012.