IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Review on CP-ABE for Big Data Access Control in Cloud Computing

Ruchika Katariya[1*], Amit Dangi[2]

[1,2]Dep. of Computer Science & Engineering, Mandsaur University, Mandsaur, M.P, India

Corresponding Author: ruchika.katariya@meu.edu.in

DOI: https://doi.org/10.26438/ijcse/v7i4.941943 | Available online at: www.ijcseonline.org

Accepted: 22/Apr/2019, Published: 30/Apr/2019

***Abstract*:-** Cloud computing be a model for enabling on-demand network access to a collective pool of configurable computing resources that can be rapidly released. Cloud attempt adjustable and cost effective repository for big data but the major problem is to deal with big data access control. classical encryption techniques are used for confidentiality and integrity over transmitted data. ABE is a fascinating explication for data access control in cloud. ABE methods encrypt attributes to a certain extent than the whole data. This paper comparative surveys the possibility of different ABE methods.

***Keyword*:** Access Control, Key Policy Attribute Based Encryption, Ciphertext Policy Attribute Based Encryption, Hidden Policy Attribute Based Encryption

I. INTRODUCTION

Cloud computing is a kind of deploying of computer programs and high level services. By means of cloud computing, users are capable in the direction of right to use software in addition to applications commencing anywhere they are. Cloud computing provides a simple way to access server, database over the internet. Accumulating conscious data on untreated servers is asserting issue for this model.
Applications so as to scuttle in the cloud can balance several factors including size of data, load balancing, bandwidth, and security. Solitary of the chief barriers toward cloud espousal be facts protection as well as isolation, since the facts vendor as well as the overhaul supplier be not inside the identical trusted sphere. Protection issues be more and more momentous inside minor coating transportation as a Service (IaaS) to higher Platform as a Service (PaaS). These cloud layers be inside deployed models (public, private, community, and hybrid) in high end Mobile Cloud Computing (MCC).

Cloud attempt adjustable and cost effective repository for big data but the major problem is to deal with big data access control. Encryption techniques are used to solve the problem of access control. Attribute-Based Encryption (ABE) is recently make-believe public key cryptographic method so as to mechanism inside a one-to-many manner as well as be moreover called fuzzy encryption. Public key encryption methods amass encrypted facts on top of third revelry servers, even as distributing decryption keys toward approved users. Though, here be a lot of drawbacks toward this. Primary, it be hard toward proficiently direct the allotment of secret keys to approved users. Next, here is a need of suppleness as well as scalability. Third, facts owners have got to be online at any time encrypting or re-encrypting facts, otherwise distributing the secret keys.

II. LITERATURE REVIEW

Let's look at works that is already done by various researchers Suchitra Khuntia, P. Syam Kumar.[1] The Author proposed CP-ABE for data access control. Applied mask techniques to hide attributes. Decreases computational overhead of encryption and decryption than existing schemes.

Ms. Yogita S. Gunjal, Mr. Mahesh S. Gunjal, Mr. Avinash R. Tambe.[2] In this paper author proposed two ABE methods i.e. KP-ABE(Key-Policy Attribute Encryption) and CP-ABE(Cipher-text Policy Attribute Based Encryption). Using algorithms minimizes the beyond confines via plummeting the announcement in the clouds of the internet and rising scalability, suppleness, as well as fine-grained admittance be in command of huge range systems.

Shweta Kaushik, Charu Gandhi. [3] Author proposed a hybrid symmetric encryption/ decryption algorithm for safe facts storage at cloud server. The key used for decryption process is shared with official user only. By using the hybrid symmetric encryption algorithm DO is ensured so as to it provides extra security for its data and user is ensured that data retrieved by him is intact without any access of intruders.

Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood, and AtaUllah Ghafoor.[4] Author widely survey each and every ABE scheme as well as creates a comparison table for the key criteria for these schemes in cloud applications.

III. ANALYTICAL REVIEW OF KP-ABE, CP-ABE, HP-CP-ABE SCHEMES

KP-ABE: Key-policy attribute-based encryption (KP-ABE) is a significant type of ABE method. KP-ABE uses private key to encrypt sender's message. KP-ABE also uses some set of attributes to transfer sender's data securely from one end to another end. In this method access structure is very important that defines key holder will decrypt which ciphertexts.

KP-ABE method uses four algorithms:

1. *Setup:* This algorithm is based on two parameters pk & mk. PK is used to encrypt the sender's message ans MK is used to cause users confidential key.
2. *Encryption:* This algorithm takes a message M, the Public key PK, and a set of attributes as input. It outputs the ciphertext E.
3. *Key Generation*: Access structure and a master key is used in this methods as an consideration. A confidential key produces as a return to decrypt a message.
4. *Decryption:* It takes as input the user's secret key SK for Access structure T and the ciphertext E. This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

CP-ABE: CP-ABE is public key encryption method that is used for encryption and decryption on users data coherent to users attribute. For tailored consent in cloud computing, to hand over gain control and preserve data security by defeat computing cost and to accomplish security against chosen-plain text barrage a system called CP ABE is developed.
CP-ABE method uses four algorithms:

1. *Setup:* It takes only explicit security parameter and produces two parameter first the public parameters 'PR' and second is master key 'MR'.
2. *Encrypt (PR, m, a):* In this algorithm, the parameter used are: the public parameters 'PR', message 'm', and 'a' the access structure. The encryption algorithm will encrypt message 'm' and give a cipher text 'ct'. A cloud user can access the structure and decrypt the message if he has a set of attributes that satisfies the access structure.
3. *Key Gen (MR, s):* In this algorithm first parameter is the master key 'MR' and second is set of attributes's' that define the key. It gives the outputs in private key 'sk'.
4. *Decrypt (PR, ct, sk):* In this algorithm, the parameters 'PR'(public parameter) and 'ct' (cipher-text) are taken as inputs to provide control access policy 'a', and 'sk' is a private key for a set of attributes 's'. If the set 's' of attributes gives the access structure 'a' then the algorithm will decrypt 'ct' and return the message 'm'.

HP-CP-ABE: Hidden policy CP-ABE method is based on multi secret sharing scheme. HP-CP-ABE method is very important in some requisition for transferring data from one end to another end. It assures that user can describe their policies flexibly.
HP-CP-ABE method uses four algorithms:

1. *Setup*: In this algorithm a security parameter K is used as an input and generate public key pk and master key mk on the basis of attribute set and bilinear group.
2. *Keygen*: This algorithm takes attribute set w and a master key mk as an input and produces a secret key sk.
3. *Encrypt*: This algorithm encrypt message m where m belongs to bilinear group. This algorithm is based on access tree, it selects a random element and assign it to tree based access policy and returns the cipher text.
4. *Decrypt*: this algorithm takes cipher text as an input and apply users private key to decrypt the users message.

IV. COMPARISION OF ACCESS MODELS

Parameters	KP-ABE	CP-ABE	HP-CP-ABE
Access permission count	Less	Average	Good
Fine grained access control	Low, No longer flexible	Average of complex access control	More access control in certain applications
Efficient	Average, Good in broadcast encryption	Average, Not efficient some times	More efficient in most applications
Confidential	Sometimes don't know who can decrypt the encrypted data	Customize authorization	Protect personal data in private cloud

Key Policy Attribute Based Encryption (KP-ABE) scheme is plan for one-to-many conversation. KP-ABE design is relevant for analytical systems. In this Scheme encryptor cannot resolve who can decrypt the encrypted data. Encryptor can isolated adopt descriptive attributes for the input, and has no elite but to faith the key issuer. This policy is average in efficiency but good in broadcast encryption. Sometimes it may have no longer fine grained access control. hidden policy CP-ABE scheme is stationed on compound structure bilinear faction and linear secret splitting scheme. This scheme hand over CPA protected with four quarrel hypothesis. hidden policy CP-ABE design is

uasge for profitable big data entree authority with confidentiality retain design. In comparision with CP-ABE policy HP-CP-ABE Policy is more efficient and has good in access permission count also more access control in certain application.

V. CONCLUSION

In this manner, ABE methods are efficient for big data access because it provide secure access with minimum time so it has low cost. In our comparison HP-CP-ABE policy uses tree based access structure to provide flexibility. Though HP-CP-ABE method is more secure and efficient in comparison with others. Cloud computing has lots of scope in future. Some new ABE methods may introduce that are more efficient and reliable.

REFERENCES

[1] Ms. Yogita S. Gunjal, Mr. Mahesh S. Gunjal, Mr. Avinash R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing", IEEE 2018 International Conference On Advances in Communication and Computing Technology (ICACCT)

[2] Sucharita Khuntia, P. Syam Kumar, "New Hidden Policy CP-ABE for Big Data Access Control with Privacy-preserving Policy in Cloud Computing", IEEE – 43488.

[3] Parmar Vipul Kumar, RajaniKanth Aluvalu, "Key Policy Attribute Based Encryption (KP-ABE):A Review", International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 2, 2015

[4] Shweta Kaushik, Charu Gandhi, "Cloud data security with hybrid symmetric encryption", IEEE 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)

[5] Umesh Chandra Yadav and Syed Taqi Ali, "Ciphertext Policy-Hiding Attribute-Based Encryption", IEEE 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)

[6] Runhua Xu, Yang Wang, Bo Lang, "A Tree-Based CP-ABE Scheme with Hidden Policy Supporting Secure Data Sharing in Cloud Computin", 2013 International Conference on Advanced Cloud and Big Data (CBD)

[7] Ho Hui Chung, Peter Shaojui Wang, Te-Wei Ho, Hsu-Chun Hsiao, Feipei Lai, "A Secure Authorization System in PHR based on CP-ABE", The 5th IEEE International Conference on E-Health and Bioengineering - EHB 2015.

