https://doi.org/10.15623/ijret.2018.0708018 Received: 09-06-2018, Accepted: 21-07-2018, Published: 11-08-2018

IMPROVED KEY POLICY ATTRIBUTE BASED ENCRYPTION (KP-ABE)

ParmarVipulkumarJ[1], Rajanikanth Aluvalu[2]

[1]Research scholar, Department of C.E, School of Engineering, R.K. University, Rajkot
[2]Assoc. Professor, Department of C.E, School of Engineering, R.K. University, Rajkot.

Abstract

Here stays an accelerating of implementation of cloud computing between enterprise. Conversely, touching the organization and powerful record of reliable dominion of the records holder to community cloud will fake confidence and isolation risks. Records confidence and policy are the dangerous problems for distant statistics storing. A security operator compulsory data access control instrument necessity be delivered earlier cloud operators require the right to subcontract complex data storing in the cloud. By the entry of sharing personal business records on the cloud servers, it is authoritative accept and effective encryption scheme by fine grain access control to encrypt subcontracted records. KP-ABE system is planned on behalf of one to many infrastructures. KP-ABE system can be accomplish fine grain access control and more elasticity to control users. In this paper we had enhanced KP-ABE Access Control model. In our enhanced Model Encryptor can decide who can Decryptdata.

Keywords: *- Access control, Clould, KP-ABE.*

---***---

1. INTRODUCTION

In several circumstances, once a employer encodes delicate records, it is overbearing that create an exact entrance policy control on who can decrypt this data. First presented an attribute based encryption (ABE) configuration is completely based on public key cryptography.[12] Security and access control is the main aim of these copies scheme. The key phases are to Deliver litheness, scalability or fine grained access control. [7] CP-ABE is the reconstructed form of the traditional of ABE. Workers are allocated by an entrée diagram configuration over the records attributes. Establishment records are knobs of the access diagram. The elements are related to foliage nodes. To reproduce the access diagram Construction is the secret key of the customer is distinct. [4] Cipher-texts are categorized by many attribute and private keys related with monotonic entry configurations that mechanism which cipher texts are users capable to decrypt. KP-ABE system is intended for one-to-many infrastructures.[1] In KP-ABE scheme, ciphertexts are private for the source by a set of expressive elements though customer's private key is supplied via the important element specialist internments a rule that requires which cipher texts are used to decrypt the record.[15] KP-ABE systems are appropriate for organized administrations by directions about who can send exact data. Distinctive requests of KP-ABE comprise safe scientific examination and target program. E.g. In a safe methodical examination scheme, checkup record entrances could be understood with attributes such by way of the designation of the customer, the date and period of the employer exploit, and the kind of records changed or opened by the customer exploit.[14] While a medical predictor exciting with certain examination would be issued a private key that related with a precise entrance construction. The private key would only exposed inspection histories whose qualities fulfilled the access rule linked through the private key. [8] The main KP-ABE structure was providing. Which was actual complex it is allowed the entrée programs to be articulated by any monotonic scheme done encrypted records. The scheme was verified selectively safe under the Bilinear Diffie-Hellman declaration. Future, Ostrovskyet al. projected a KP-ABE system where private keys can characterize any access method done attributes, counting nonmonotone ones, by mixing reversal systems hooked on the Goyal et al. KP-ABE system. [2]

2. RELATEDWORKS

This segment analyses the idea of different attribute based encryption schemes. These systems are planned as access control tools to cloud storing.

2.1 Attribute Based Encryption(ABE)

An ABE system presented by Sahai and Waters in 2005 And the main concept of the system is to deliver to safety and ABE is based on public key for one to several encryptions that permits Customer to encrypt and decrypt records built on the elements. The secrete key of customer and the ciphertexts are depend on the elements.[16] In the system, the ciphertext decryption is probable if the set of elements of the customer key is match with ciphertext of attributes. Decryption is probable if the no of equivalent is at least threshold value *d*. Attribute Based Encryption having a crucial security feature is collision-resistance. Challenge in ABE is that its hold the various keys and only keys should be able to access data If at smallest in separate key gifts access[17].

https://doi.org/10.15623/ijret.2018.0708018 Received: 09-06-2018, Accepted: 21-07-2018, Published: 11-08-2018

2.2 Key Policy Attribute Based Encryption(KP-ABE)

KP-ABE exists the adapted form of traditional typical of ABE. cipher texts stay associated through a usual of elements and the private keys are connected with entrée arrangements on these attributes that controls which cipher text a consumer is intelligent to decrypt.[18] This access structure designates an entrance policy. The user can decrypt the file only if there is a match among access policies in the key and the attributes in the cipher text. The main weakness of this scheme is, since the access rule is assembled based on user's private key, the records holder that encryptor can't decide who is the data decryptor users. He has to conviction the main issuer[11].

2.3 Ciphertext Policy Attribute Based Encryption(CP-ABE)

CP-ABE exists additional improved form of ABE called presented by Sahai. CP-ABE workings in the converse method of KP-ABE. Cipher texts are connected with access arrangements which symbolize access policies. Private Key is connected by a set of user elements.[9] For decrypting the file, there should be contest amongst access policy in cipher text and attributes in the user's private key. Data owner has full regulator here. CP-ABE has constraints in identifying composite policies and supervision user attributes with plasticity. Also it is not much scalable and user withdrawal is inspiring[10].

3. EXISTING SYSTEM

Encryptor cannot decide who is the data decryptor user. it is choose only descriptive records, and takes no special but to belief the key generator of KP-ABE is not confidant presentations.[7] For sample, cultured program encryption, wherever customers are defined by different elements and in this, the lone whose elements equal a policy connected with a ciphertext, it can decrypt the ciphertext. KP-ABE system maintenances customer secret key responsibility. It is providing fine grained access but has no longer with flexibility and scalability[12].

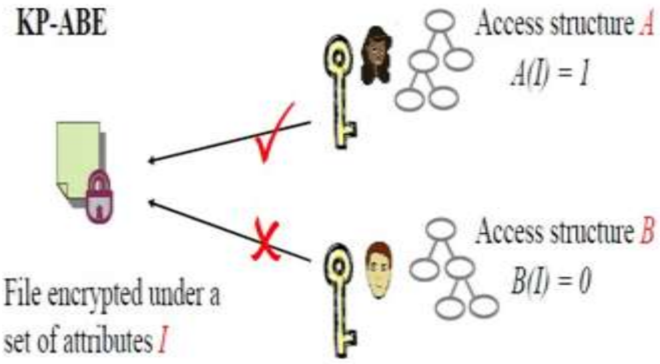

Fig 1: KP-ABE Access control

KP-ABE scheme having a ensuing four procedures: [3]:

1. ***Setup:***In this input K as asacure factor then gives PK as public key and a secret key MK. PK is used by senders for encryption. MK is used for the produce a secreat key and authority has to be identified.
2. ***Encryption:*** in this message M, and inputs are given to the public key PK, and a set of elements. And output it produced ciphertextE.
3. ***Key Generation:*** Inputs an access configuration T then the master key MK. and results a secret key SK that allow user to decrypt records or cipher-text below the attribute when matching ofT.
4. ***Decryption***: It takes as input the user's secret key SK for Structure T and the ciphertext which is encrypted with the attributs. It is gives the output of the message M if and only if the element set of the user's are match with structure T. [3]

4. OURCONSTRUCTION

Here we have defined a proposed system to solve the KP-ABE limitation. Encryptor cannot decide who is the data decryptor user. And we can solve this problem through given proposed system. In proposed system data owner generate a publickey (Pk) for encryption and decryption and also generate a MasterKey (Mk). Through the public key data owner known the the who can decrypt the data. Keygen is a trusted Authority keygen is generate a Secretekey (Sk) for decryption user decrypt the data through PublicKey (Pk) and SecreteKey (Sk). And we can also use a Multi Authority different Keygen generate a different SecreteKey (Sk) to decrypt the data.

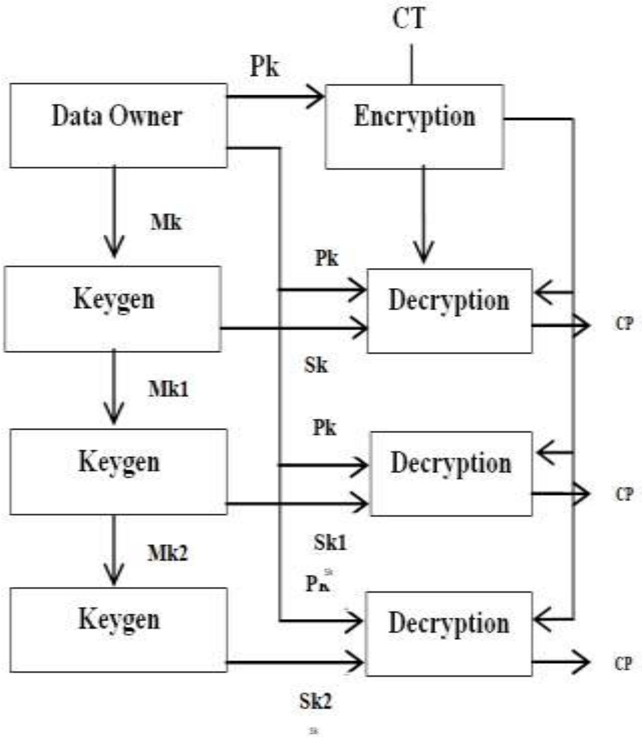

Fig 2: Our Construction

https://doi.org/10.15623/ijret.2018.0708018 Received: 09-06-2018, Accepted: 21-07-2018, Published: 11-08-2018

1. ***Setup:*** in this input K as a sacure factor then gives PK as public key and a secret key MK. PK is used by senders for encryption. MK is used for the produce a secreat key and authority has to beidentified.
2. ***Encryption:*** in this message M, and inputs are given to the public key PK, and a set of elements. And output it produced ciphertextE.
3. ***Key Generation:*** Inputs an access configuration T then the master key MK. and results a secret key SK that allow user to decrypt records or message below the attribute when matching of T[3].
4. ***Decryption:*** in this input secret key Skor public key Pk of data owners for ciphertext E and access structure T. It was encrypt below the set of attribute. This procedure produced the message M[3].

5. RESULTANALYSIS

Here segment we contemporaneous a KP-ABE access control with resolve problem that encryptor cannot choose who can decrypt the data. In planned system we can encrypt data with data owner public key and decrypt with data owner public key or secrete key generated by key generation algorithm through the public key of data owner. Data owner knows who can decrypt data. And in proposed system we have to include multi authority scheme that is data decrypt same public key but different secret keys diagram shown in figure2.

Table 1: Comparisons

KP-ABE		Enhanced KP-ABE	
Encryptor	Decryptor	Encryptor	Decryptor
X	(Y,Z)	(X, Y)	Y

In above Table 1 its gives a comparison of KP-ABE access control modal and Enhanced KP-ABE access control modal. In existing KP-ABE encryptor X and decryptor Y,Z so encryptor cannot control over the decryptor and Enhanced KP- ABE access control model encryptor X,Y and decryptor Y. so encryptor having a control ondecryptor.

6. CONCLUSION

Here, we had enhanced KP-ABE access control model which is the variation of classical model of ABE. Though KP-ABE provides security by allowing entrée programs to be conveyed by any monotonic method done encrypteddata,limitationinKP-ABEaddressedinsectionII (B) is yet to be an issue. So in our proposed system, we can resolve KP-ABE access scheme in manner such that the Data owner unable to decide who is the data accesser. It choose only rendom attributes for the data. In upcoming we have to control over the descriptive attribute user can choose the attributes.

REFERENCES

[1] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing" International Journal of Advanced Research in Computer and Communication EngineeringVol.2,Issue11,November2013.

[2] ChangjiWang1,2,3 and Jianfa Luo1,2 "An Efficient Key-Policy Attribute- Based Encryption Scheme with Constant Ciphertext Length" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 810969.

[3] Mr. Anup R. Nimje #1 , Prof. V. T. Gaikwad*2 ,Prof. H. N. Datir^3 "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" International Journal of Computer Trends and Technology- volume4Issue3-2013.

[4] John Bethencourt, AmitSahai, Brent Waters "Ciphertext-Policy Attribute- Based Encryption" Supported the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.

[5] N.krishnaL.Bhavani "HASBE A Hierarchical Attribute Set Based Encryption For Flexible Scalable And Fine Grained Access Control In Cloud Computing" International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct2013.

[6] Guojun Wang, Qin Liu, Jie Wu "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services" CCS'10, October 4–8, 2010, Chicago, Illinois, USA. ACM 978-1-4503-0244- 9/10/10.

[7] PunithasuryaK,JebaPriya S "Analysis of Different Access Control Mechanism in Cloud" International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.2, September2012.

[8] S. Gokuldev, S.Leelavathi "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May2013.

[9] Parminder Singh, Sarpreet Singh "A New Advance Efficient RBAC to Enhance the Security in Cloud Computing" Volume 3, Issue 6, June 2013 ISSN: 2277128X.

[10] Mauro José A. de Melo, Mauro José A. de Melo "A STUDY OF ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT" International Journal of Computers & Technology www.cirworld.com Volume 3 No. 3, Nov-Dec,2012.

[11] *K.Priyadarsini, C.Thirumalaiselvan "*A Survey on Encryption Schemes for Data Sharing in Cloud Computing" *(IJCSITS), ISSN: 2249-9555 Vol. 2, No.5, October2012.*

[12] SonamChugh, Sateesh Kumar Peddoju "Access Control Based Data Security in Cloud Computing" International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun2012.

https://doi.org/10.15623/ijret.2018.0708018 Received: 09-06-2018, Accepted: 21-07-2018, Published: 11-08-2018

[13] Bibin K Onankunju“ Access Control in Cloud Computing” International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013 1 ISSN2250-3153.

[14] Vamsee Mohan, M. Rajani “Attribute-Based Encryption of Scalable and Secure Sharing in Personal Health Records using Cloud Computing” International Journal of Advanced Research inComputer Science and Software Engineering Volume 4, Issue 7, July 2014 ISSN: 2277128X.

[15] Ms. Sunita*, Prachi “Efficient Cloud Mining Using RBAC (Role Based Access Control) Concept” International Journal of Advanced Research in Computer Science and Software Engineering” Volume 3, Issue 7, July 2013 ISSN: 2277128X.

[16] Kanupriyya1, Richa Sapra2 “Role-Based Access-Control Backup and Restoration Ontology “ International Journal of Advanced Research in Computer Science and Software Engineering” Volume 2, Issue 1, January – February 2013 ISSN2278-6856.

[17] Abhishek Patel, Mayank Kumar “A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module” International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN: 2277128X.