International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 19
August 2018

Cloud Assisted Attribute based Encryption for Health Monitoring System

Akula Joshitha
M.Tech(Computer Science & Engineering), Bharat Institute of Engg & Tech., Ibrahimpatan(M).R.R Dist.
P. Srinivas Rao, M.Tech
Associate Professor, Dept of CSE, Bharat Institute of Engg & Tech., Ibrahimpatan(M).R.R.Dist.

Abstract:*Cloud computing is an emerging computing paradigm, enabling users to store their data remotely in a server and toprovide services on-demand. In cloud computing, cloud users and cloud service providers are almost clear fromdifferent trust domains. The critical issues for remote data storage are data security and privacy.The shared data files in most cases have the features of multilevelhierarchy, specifically in the area of healthcare and the military. However, the hierarchy system of shared files hasnot been explored in CP-ABE. In this paper, an effective file hierarchy attribute-based encryption method isproposed in cloud computing. The layered access structures are included into a single access structure, and then,the hierarchical files can be encrypted with the integrated access structure. The cipher text components similar toattributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is preserved.Moreover, the proposed scheme is proved to be secure under the entire assumption.*

Keywords-Attribute-based encryption, cipher text policy, fine-grained access control, re-encryption.

I. INTRODUCTION

In cloud computing, to protect data from leaking, usersneed to encrypt their data before being shared. Accesscontrol [6], [7] is paramount as it is the first line of defensethat prevents unauthorized access to the shared data. Withthe burgeoning of network technology and mobile terminal,online data sharing has become a new “pet”, such asFacebook, MySpace, and Badoo. Meanwhile, cloud is oneof the most promising application platforms to solve theexplosive expanding of data sharing. In cloud computing, toprotect data from leaking, users need to encrypt their databefore being shared. Access control is paramount thatprevents unauthorized access to the shared data. Recently,attribute-based encryption (ABE) has been attracted muchmore attentions since it can keep data privacy and realizefine-grained ,one-to-many n,and non interactive accesscontrol. Ciphertext-policy attribute based encryption (CPABE) is one of feasible schemes which has much moreflexibility and is more suitable for general applications.In cloud computing, authority accepts the userenrollment and creates some parameters. Cloud ser-viceprovider (CSP) is the manager of cloud servers and providesmultiple services for client. Data owner encrypts anduploads the generated ciphertext to CSP. User downloadsand decrypts the interested ciphertext from CSP. The sharedfiles usually have hierarchical structure. That is, a group offiles are divided into a number of hierarchysubgroups located at different access levels. If the files inthe same hierarchical structure could-based encrypted by anintegrated access structure, the storage cost of ciphertext andtime cost of encryption could be saved.

II. RELATED WORK

Attribute Based Encryption (ABE): An attribute based encryption scheme introduced bySahai and Waters in 2005 and the goal is to providesecurity and access control. Attribute-basedencryption (ABE) is a public-key based one to manyencryptions that allows users to encrypt and decryptdata based on user attributes. In their context, the roleof the parties is taken by the attributes. Thus, theaccess structure will contain the authorized sets ofattributes. They restrict the attention to monotoneaccess structures. However, it is also possible to(inefficiently) realize general access structures usingthe techniques by having the not of an attribute as aseparate attribute altogether. Thus, the number ofattributes in the system will be doubled. From now on,unless stated otherwise, by an

access structure wemean a monotone access structure.

An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms.

Setup: This is a randomized algorithm that takes no inputother than the implicit security parameter. It outputsthe public parameters PK and a master key MK.

Encryption: This is a randomized algorithm that takes as input amessage m, a set of attributes γ, and the publicparameters PK. It outputs the ciphertext E. KeyGeneration This is a randomized algorithm that takesas input – an access structure A, the master key MKand the public parameters PK. It outputs a decryptionkey D.

Decryption: This algorithm takes as input – the ciphertext E thatwas encrypted under the set γ of attributes, thedecryption key D for access control structure A andthe public parameters PK. It outputs the message M ifγ ∈ A.The problem with attribute based encryption (ABE)scheme is that data owner needs to use everyauthorized user's public key to encrypt data. Theapplication of this scheme is restricted in the realenvironment because it use the access of monotonicattributes to control user's access in the system.

Cipher Text Policy Attribute Based Encryption

Another modified form of ABE called CP-ABEintroduced by Sahai. In a CP-ABE scheme, everyciphertext is associated with an access policy onattributes, and every user's private key is associated

with a set of attributes. A user is able to decrypt aciphertext only if the set of attributes associated with

the user's private key satisfies the access policyassociated with the ciphertext. CP-ABE works in thereverse way of KP-ABE. The access structure of thisscheme or algorithm , it inherit the same method whichwas used in KP-ABE to build. And the access structurebuilt in the encrypted data can let the encrypted datachoose which key can recover the data, it means theuser's key with attributes just satisfies the accessstructure of the encrypted data. And the concept of thisscheme is similar to the traditional access controlschemes. The encryptor who specifies the thresholdaccess structure for his interested attributes whileencrypting a message. Based on this access structuremessage is then encrypted such that only those whoseattributes satisfy the access structure can decrypt it. themost exiting ABE schemes are derived from theCPABE scheme.

CP-ABE scheme consists of following fouralgorithms:

Setup

This algorithm takes as input a security parameter Kand returns the public key PK as well as a systemmaster secret key MK. PK is used by message sendersfor encryption. MK is used to generate user secret keysand is known only to the authority.

Encrypt

This algorithm takes as input the public parameter PK,a message M, and an access structure T. It outputs theciphertext CT.

Key-Gen

This algorithm takes as input a set of attributesassociated with the user and the master secret key MK.It outputs a secret key SK that enables the user todecrypt a message encrypted under an access tree

structure T if and only if matches T.

Decrypt

This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns themessage M if and only if satisfies the access structure

associated with the ciphertext CT.It improves the disadvantage of KP-ABE that theencrypted data cannot choose who can decrypt. It cansupport them access control in the real environment.In addition, the user's private key is in this scheme, acombination of a set of attributes, so an user only usethis set of attributes to satisfy the access structure inthe encrypted data. Drawbacks of the most existingCP-ABE schemes are still not fulfilling the enterpriserequirements of access control which requireconsiderable flexibility and efficiency. CP-ABE haslimitations in terms of specifying policies andmanaging user attributes. In a CP-ABE

scheme,decryption keys only support user attributes that are
organized logically as a single set, so the users canonly use all possible combinations of attributes in asingle set issued in their keys to satisfy policies. After
that ciphertext-policy attribute set based encryption(CP-ASBE or ASBE for short) is introduced byBobba, Waters et al [7]. ASBE is an extended form ofCP-ABE. It organizes user attributes into a recursiveset based structure and allows users to imposedynamic constraints on how those attributes may becombined to satisfy a policy. The CP-ASBE consistsof recursive set of attributes. The challenge inconstructing a CP-ASBE scheme is unselectivelyallowing users to combine attributes from multiple setswithin a given key. There is challenge for preventingusers from combining attributes from multiple keys.

Hierarchical attribute-based Encryption

This scheme Hierarchical attribute-based encryption(HABE) is derived by Wang et al The HABE modelconsists of a root master (RM) that corresponds to the
third trusted party (TTP),multiple domain masters(DMs) in which the top-level DMs correspond tomultiple enterprise users, and numerous users thatcorrespond to all personnel in an enterprise. Thisscheme used the property of hierarchical generation ofkeys in HIBE scheme to generate keys. Then, HABEscheme is defined by presenting randomized
polynomial time algorithms as follows:

Setup

(K)→(params,MK0): The RM takes a sufficientlylarge security parameter K as input, and outputssystem parameters params and root master key MK0.

CreateDM(params,MKi, PKi+1) → (MKi+1): Whether the RMor the DM generates master keys for the DMs directlyunder it using params and its master key.

CreateUser

(params,MKi, PKu, PKa) → (SKi,u, SKi,u,a):The DMfirst checks whether U is eligible for a, which isadministered by itself. If so, it generates a user identitysecret key and a user attribute secret key for U, usingparams and its master key; otherwise, it outputs“NULL”.

Encrypt

(Params; f ;A; {PKa|a E A})→(CT): A user takes a filef, a DNF access control policy A, and public keys ofall attributes in A, as inputs, and outputs a ciphertextCT.

Decrypt

(Params, CT, SKi,u,{SKi,u,a|aECCj}→(f):Auser,whose attributes satisfy the j-th conjunctiveclause CCj, takes params, the ciphertext, the useridentity secret key, and the user attribute secret keys
on all attributes in CCj, as inputs, to recover theplaintext.This scheme can satisfy the property of fine grainedaccess control, scalability and full delegation. It canshare data for users in the cloud in an enterpriseenvironment. Furthermore, it can apply to achieveproxy re-encryption [4]. But in practice, it is
unsuitable to implement. Since all attributes in oneconjunctive clause in this scheme may be administeredby the same domain authority, the same attribute maybe administered by multiple domain authorities.

Key Policy Attribute Based Encryption (KP-ABE)

It is the modified form of classical model of ABE.Users are assigned with an access tree structure over
the data attributes. Threshold gates are the nodes of theaccess tree. The attributes are associated by leaf nodes.To reflect the access tree Structure the secret key ofthe user is defined. Ciphertexts are labeled with sets ofattributes and private keys are associated withmonotonic access structures that control whichciphertexts a user is able to decrypt. Key PolicyAttribute Based Encryption (KP-ABE) scheme isdesigned for one-to-many communications.KP-ABE scheme consists of the following fouralgorithms:

Setup

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 19
August 2018

Algorithm takes input K as a security parameter and returns PK as public key and a system master secretkey MK.PK is used by message senders forencryption. MK is used to generate user secret keysand is known only to the authority.

Encryption

Algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.

Key GenerationAlgorithm takes as input an access structure T and themaster secret key MK. It outputs a secret key SK thatenables the user to decrypt a message encrypted undera set of attributes if and only if matches T.

Decryption

It takes as input the user's secret key SK for accessstructure T and the ciphertext E, which was encrypted

under the attribute set. This algorithm outputs themessage M if and only if the attribute set satisfies the

user's access structure T.The KP-ABE scheme can achieve fine-grained accesscontrol and more flexibility to control users than ABEscheme. The problem with KP-ABE scheme is theencryptor cannot decide who can decrypt theencrypted data. It can only choose descriptiveattributes for the data, it is unsuitable in someapplication because a data owner has to trust the keyissuer.

III. PROPOSED WORK

To find ranked search for effective utilization of outsourced cloud data under the aforementioned model, our system design shouldsimultaneously achieve security and performance guarantees as follows.

1. Multi – keyword Ranked Search : To implements search schemes which access multi – keyword query and provide resultsimilarity ranking for effective data retrieval.

2. Efficiency : This also perform privacy should be achieved with low communication and comp.

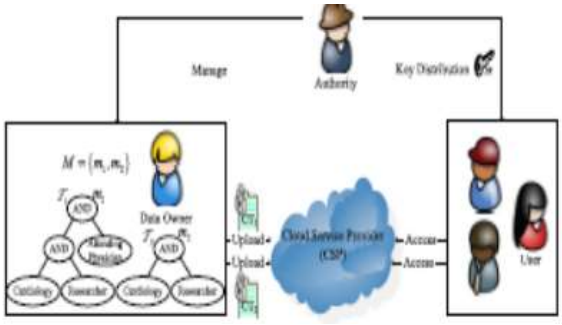

Fig.1An example of FH-CP-ABE scheme used in cloudcomputing

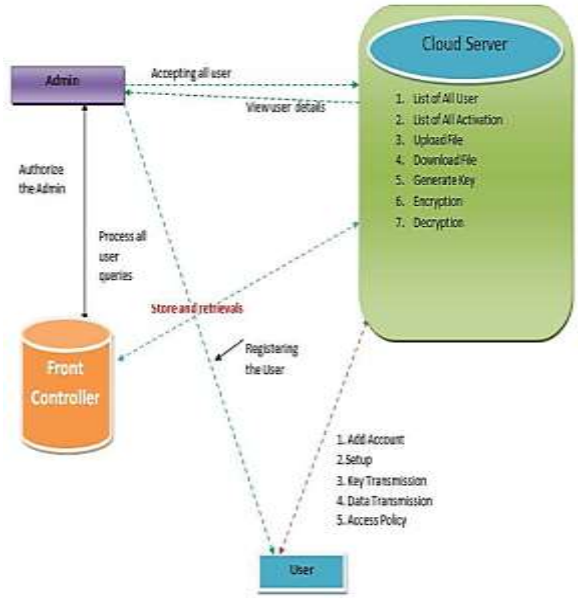

Fig.2 System Architecture

Data Owner:

Register with cloud server and login (username must be unique).Send request to Key transmission to generate ABEKey on the user name. Browse file and request Private Key to encrypt the data, Upload data to service provider.Verify the data from the cloud.

Public Key Generator (Key Transmission):

Receive request from the users to generate the Key, Store all keys based on the user names. Check the username andprovide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud server and un revokethe user after updating the

private key for the corresponding file based on the user).

End User:

1. In this module receiver first has to Register and login, Request secret key, Request available files in the cloud andreceive files.
2. Every key come respective unique id.

Data Sharing:

1. Data Share group wise as per authorized account.
2. Every File key changeable.

Set theory : Let S = I,P,R,O,K

- Where,
- S: Public integrity auditing system.
- I: Set of inputs.
- P: Set of processes.
- R: Rules or constraints.
- K: Keyword
- O: Set of outputs/Final output.
- I = i1, i2,.....,in
- Where,
- i1,i2,...,in = Files shared by the users.
- P=p1, p2, p3, p4, p5, p6, p7
- Where,
- p1: Key generation
- p2: Generate commitment string
- p3: Open
- p4: Verify
- p5: Update.
- p6: Proof Update.
- R = r1
- Where,
- r1: Revoked user should not be able to access files shared by users.
- r2: Proper keyword should be extracted.
- Where,
- O1: Valid user cloud access any file.

Output:-

- Result(Z) ={In,Pn,Rn}
- In->i1,i2,i3,.....in(Share file)
- Pn-> p1,p2,p3,....pn(process)
- Rn-> r1,r2,r3.....Rn(Revocation)
- Result(Z) = {pi, 0<I<k}.....set of probability
- ~Result(Z) = {pi,(K,mi),{false otherwise}}
- here , K(Z) = {ki, 0<I<n} Set the keyword.

ion.

IV. CONCLUSION

The hierarchical files are encrypted with an integrated access structure and the cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is saved. The proposed schemehas an advantage that users can decrypt all authentication files by computing secret key once. Thus, the time cost of decryption as also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to besecure under DBDH assumption.

REFERENCES

[1] C.-K. Chu ,W.-T. Zhu, J. Han, J. –K. Liu, J. Xu, and J. Zhou, Security concerns in popular cloud storageservices, IEEE Pervasive Computing., vol.12,no.4,pp.5057,Oct./Dec.2013.

[2] T. Jiang , X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, TIMER: Secure and reliable cloud storage against datare-outsourcing, in Proc. 10th Int. Conf. Inf. Secure.Pracr.Exper.,vol.8434.May 2014,pp.346358.

[3] K. Liang, J. K.. Liu, D. S. Wong, and W. susilo, An efficient cloud based revocable identity-based proxy reencryption scheme for public clouds data sharing, in Proc.19th Eur.Symp.Res.Comput.Secure.,vol.8712.Sep .2014,pp.257272.

[4] T.H. Yuen, Y. Zhang, S.M. Yio, and J.K. Liu, Identity-based encryption with post-challenge auxiliary inputs forsecure cloud applications and sensor networks, in Proc. 19th Eur.Symp. Res. Comput. Secure., col.8712.Sep.2014,pp.130147.

[5] K. Liang et al., A DFA-based functional proxy re-encryption scheme for secure public cloud sharing, IEEETrans. Inf. Forensics Security, vol.9, no.10, pp.16671680, Oct.2014.

[6] T.H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, k-times attribute-based

anonymous accesscontrol for cloud computing, IEEE Trans.Comput.,vol.64,no.9,pp.25952608,Sep.2015.

[7] J.K. Liu, M.H. Au, X. Hiang ,R. Lu, and J. Li, Fine-grained two factor access control for Web-based cloudcomputing services, IEEE Trans. Inf. Forensics Security,vol.11,no.3,pp.484497,Mar.2016.

[8] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryptology. Berlin, Germany:Springer, May 2005, pp.457473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control ofencrypted data, in Proc.13th ACM Conf. Comput. Commun. Secur., Oct.2006,pp.8998.

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, Efficient attribute-based encryption from R-LWE, Chin. J.Electron., vol.23, no.4, pp.778782, Oct.2014.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007,pp. 321–334.

[12] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"

in Proc. 14th ACM Conf. Comput. Commun. Secur., Oct. 2007,pp. 456–465.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediatedciphertext-policy attribute-based encryption and its application," in Proc.10th Int. Workshop Inf. Secur. Appl., Aug. 2009, pp. 309–323.

[14] X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policyattribute-based access control towards revocation in cloud computing,"J. Universal Comput. Sci., vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[15] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan,"CP-ABE with constant-size keys for lightweight devices," IEEE Trans.Inf. Forensics Security, vol. 9, no. 5, pp. 763–771, May 2014.