Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Efficient Attribute Based Encryption using File Hierarchy scheme in Cloud Computing

[1]Navya N P, [2]Ramya B, [3]Swetha V S, [4]Tejaswini J, [5]Sebin Joy, [6]Susan George

Abstract

Cipher text policy, is used to solve many problems related to the data security. Cipher text policy mainly deal with encryption based on attributes. When the data is uploaded on to the cloud, there is a chances of hacking or leakage of data.so, in this we avoid a security to the ,by using this, the key is generated by the authority for the security purpose. The proposed scheme is highly efficient where data leaking and unauthorized access to the third user is not possible, the advantages of our scheme become more efficient.

Keywords- Searchable encryption, time control, conjunctive keywords, e-health, resist offline keyword Guessing attack.

Introduction

Web based sharing information has turned out to be old, however giving security to the information is a new, "pet, for example, Watsapp, Skype, Facebook. In this, distributed computing are the best stages to take care of the issues concerning the information sharing.

In distributed computing, to shield information from spilling or unapproved access to the third client, clients need to encode their information before transferring on to the cloud. Cloud specialist organization (CSP) is the chief of cloud and gives administration to the customers. Ciphertext arrangement is one of the doable which has a great deal greater adaptability and it is more reasonable for general applications. Information proprietor scrambles the information (the information is changed over into figure content) and the encoded information is transferred on to the server, then supplier ciphertext to CSP. Presently, client downloads the encoded information and decodes the vital ciphertext from the csp. The record which has been shared progressive structure. The gatherings of documents are partitioned into various progressive subgroups situated at various level

Here let us take the military record(MR)for case, To safely share the MR data in cloud, the data separates the military data n1 that may contain the close points of interest or some other issues identified with the military. The military record n2 which doesn't contain any touchy points of interest. At that point the client embraces ciphertext approach to encode the data n1 and n2 by various get to policies utilizing diverse characteristics.

At that point the client fulfills every one of the qualities given by the proprietor, the demand is sent to the expert. In the event that it is genuine then the expert produces the token as for the client ID.

Clients encode the message and transfer to the cloud then utilizing this token produced by the specialist the client can decode the message. On the off chance that the non-client tries to get to the information more than twice then that client will be blocked and the proprietor gets the warning message.

OUR CONTRIBUTION: In this, an effective encryption in light of layered model of the strategy structure and is proposed in cloud , that is called as ciphertext utilizing document chain of command outline. The progressive structure of get to arrangement is to accomplish adaptable and proficient outcome.

The commitments of our plan are four viewpoints:

•Firstly ,we unravel the multilevel record various leveled structure utilizing characteristics and sensible operators(AND and additionally).

•Secondly ,in the wake of illuminating every one of

the properties given by the proprietor then the demand is sent to the specialist for the key era.

•Thirdly ,after the key era the message is scrambled and transferred on to the cloud by illuminating all the property tree structure the client can unscramble the information of the separate proprietor.

•Lastly, if the non-client tries to get to the information then the client neglects to explain the get to arrangement structure. The non-client will be blocked on the off chance that he attempted more than twice and the notice is sent to the proprietor.

PRELIMINARIES

Documentations utilized as a part of the work are talked about in this piece of the module, They are to be specific Access structure, Bilinear maps, DBDH supposition and Hierarchcal get to tree.

1.Access structure:

Provide the arrangement of gatherings a chance to be indicated as,{P1,P2,P3.....,Pn},And get on to structure, it is an accumulation of non-purge subsets meant by 'A', where Ac2{P1,...,Pn} which is monotone ∀B,C if B ∈ An and B ⊆ C then C ∈ A.

A non-exhaust gathering sets in accumulation An is called approved Sets.

Get to structure contains the approved sets and qualities portrays the information client.

Get to structure with monotone frame is the key idea utilized by our plan.

2.Bilinear maps:

On the off chance that e: G0XG0—>GT is a bilinear mapping where G0 and GT is a two gathering of prime having request p, and g is the generator of G0,satisfies the accompanying conditions,

Bilinearity: Function which joins the two vector spaces components that respects third vector space component.

Give u,v a chance to be any two vector spaces and Let G0 be the gathering of prime,

u, v ∈ G0 and a, b ∈ Zp, it has e(ua, vbb) = e(u, v)ab.

Non-degeneracy:If u,v ∈ G0 ,gathering of prime having request g,such that e(u,v)≠1.

Compitability:For all (u,v)∈ G0,there exists a productive calculation e(u,v).

3.DBDH presumption:

In the light of the security parameter of the system, challenger picks up a prime gathering G0 with the request p.

By haphazardly picking a,b,c∈ Zp and the generator of G0 is g.With (g,ga,gb,gc) a legitimate tuple e(g,g)abc∈ GT which is ought to and should be recognized by foe from an arbitrary component R∈ GT.

4.Hierarchical Access Tree

The Access structure is with the tree structure which contains the root level and also the get to level, forming Hierarchical Access Tree. Give 'T' a chance to be the root level get to tree that is partitioned into "k" get to levels.

Let (x,y) means the hubs of the tree, where x is the hub's line in T through and through and y is the hub's segment in T from left to right.

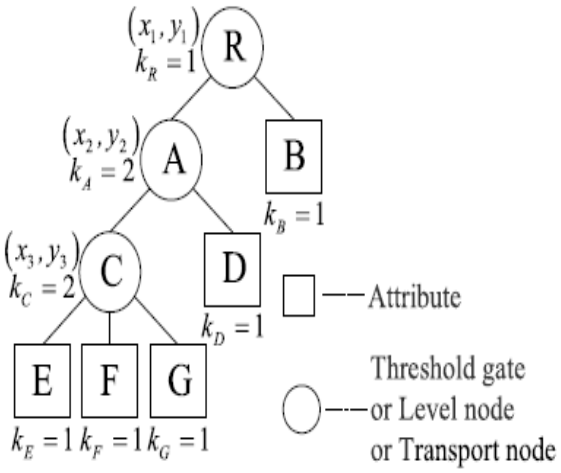


Fig. 3. An example of three-level access tree.

The hubs in the fig., can be indicated as takes after:

R=(1,1),A=(2,1),B=(2,2),C=(3,1),D=(3,2),E=(4,1),F=(4,2),G=(4,3).

E. Meaning of the framework and our development essentials.

The primary framework is separated into four unique elements:

Specialist, Cloud Service supplier ,information

proprietor and client.

Suppose, the information proprietor will be furnished with all the k documents and also with k levels and M=fm1,:::mkg is divided in distributed computing with m1 being most elevated highest order and m2 being least progressive system. The needed requirement is, m1 decoded by the client then m2:: mk can likewise be unscrambled by a similar client.

•Authority: An expert substance can be totally trusted and in the distributed computing that acknowledges the enlistment of the client. Setup and era if key operations are executed by this element.

•Cloud Service provider(CSP):CSP is halfway trusted or semi-trusted entity.Task relegated to the CSP are performed genuinely which gives back the correct results.Storage administrations for ciphertext and transmission administrations are given by Cloud specialist organization.

• Data Owner:This substance contains the gigantic information that requirements to put away and partaken in the cloud system.Defining a get to structure and execution of an Encryption operations are done through this entity.Generated Ciphertext after the execution of the Encryption operation is transferred to the CSP utilizing information proprietor.

• User:The tremendous information transferred to the cloud by the information proprietor element needs to be gotten to by the end user.Ciphertext comparing to the information is first downloaded by the entity,upon this decoding operation is performed on to that ciphertext to get back the first information.

The preparing of documents is finished by the information owner,processing makes the accompanying strides:

k content keys fck1,:::,ckkg are choosen first by the information proprietor then the Encryption procedure utilizing symmetric encryption calculation is connected on records fm1,:::,mkg with substance keys.Symmetric encryption utilized here is to be specific DES,AES.

Utilizing FH-CP-ABE encryption calculation the information proprietor encodes fck1,:::ckkg.

The ciphertext acquired after encryption is indicated as Eck(M)=f Eck(m1),::: Eck(mk)g.After utilizing encryption calculation a coordinated ciphertext of substance keys C T is gotten.

Unscrambling process makes in taking after strides:

Utilizing FH-CP-ABE unscrambling operation the client substance decodes the CT ciphertext and gets the substance key.Then utilizing symmetric unscrambling calculation the client can get the record with substance key.

The four operations that has been completed by FH-CP-ABE plan is :

Setup, KeyGen, Encrypt and Decrypt.The depiction of the operations are given underneath:

1)Setup(1k) (PK,MSK):let k be the security parameter taken by the probalistic operation and that yields in broad daylight key PK and ace key MSK.

2)(SK) KeyGen (PK ,MSK,S):the contribution to the operation is the general population key(PK),master key(MSK),and S set of properties alongside the making of emit key(SK).

3)(CT) Encrypt(PK, ck,A). contributions to the operation is Public key PK,

ck = {ck1, . . . , ckk }, and a various leveled get to tree

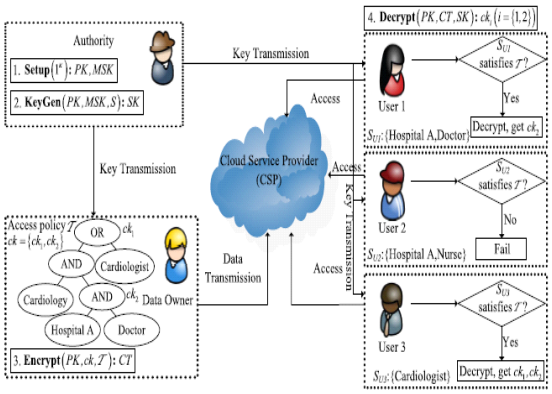
An at long last that yields in an incorporated ciphertext of substance keys CT.

4)(cki (i ∈ [1, k])) Decrypt(PK,CT, SK). This

calculation takes open key PK and Ciphertext CT which incorporates An a coordinated get to structure and an arrangement of characteristics S depicts Secrete key SK.If the piece of An is coordinated by the S set of traits, a portion of the substance keys cki (i ∈ [1, k]) can be unscrambled. On the off chance that the arrangement of traits S is coordinated by the entire get to structure A,entire content keys can be unscrambled.

The matching records mi (i ∈ [1, k]) with the symmetric unscrambling calculation can be decoded with the substance keys.

A case of FH-CP-ABE is appeared in underneath fig..



In expansion to this features,FH-CP-ABE plot gives if a two various leveled documents m1 and m2 are shared by similar information proprietor then encryption should be possible by arbitrarily picking two substance keys ck1 and ck2,{Eck1 (m1), Eck2 (m2)} is the produced ciphertexts under T the get to policy.By encryption operation get to strategy T makes an incorporated ciphertext CT and transfers ciphertext to the Cloud Service Provider CSP.

Unscrambling happens once if the client needs to get to the documents that are as of now conveyed in the cloud.Firstly the {Eck1 (m1), Eck2 (m2)} ciphertexts and CT are downloaded from Cloud Service Provider CSP.If some part or entire piece of the get to strategy T is fulfilled by end client's arrangement of attibutes decoding of a few or entire substance keys can be decoded separately.

The propose FH-CP-ABE SCHEME

In this piece of paper we have clarified the development of FH-CP-ABE in detail, as indicated by that development encryption handle for FH-CP-ABE is done, this is done as favorable position to lessen computational many-sided quality, here we clarify about the elements.

Conspire construction: We utilize a bilinear guide i,e the cross result of G0 gives GT and G0 be the prime request p of bilinear gathering and the arrangement of traits utilized A={a1,22… … } and has a generator ge, for any key has a place Zp.

Setup stage: the operation is controlled by specialist that takes the information key which is a security parameter and two irregular numbers are choosen alpha and beeta has a place with Zp , the aftereffect of this progression is people in general key(PK),master key(MSK) .

Key era stage: here we utilize open key, ace key, mystery key, specialist executes calculation where the mystery key (SK) is made utilizing the arrangement of characteristics S. The information proprietor shares n records with n get to levels, then the relating content key (ck) are encoded as an encryption procedure

encryption handle :incorporates open key substance key and the get to tree (T) tthese are taken as an info the yield of this is scrambled information called the ciphertext(CT) Polynomial structure decide : it says that polynominal values should be added to each hub the hubs are seleced arbitrarily in start to finish approach and the degee and the degree is doled out as K-1 where K is limit esteem. From the root hub R, the proprietor sets the root hub as 0 and start to finish approach the number gets slipping request there are two sorts of hubs they are level hub are the subnodes or the kids hubs alternate hubs are haphazardly chosen in outstanding hubs. In the tree structure (T) let x be a vehicle hub it demonstrates to us the way from which it transport hub it demonstrates to us the way from which it transports to the various hubs

Unscrambling: prepare incorporates open key ciphertext and mystery key this is like that of CP-ABE, which is a recursive operation if the ciphertext was a leaf hub it would have straightforwardly decoded in the event that it was a non-leaf hub then some coordination are done to discover the excat hub and this is repeted and unscrambling is finished.

FH-CP-ABE SCHEME WITH IMPROVED ENCRYPTION

It is used to reduce the computational complexity. the nodes present in the ciphertext is removes if no information us present the information only exists un leaf node not in the level node transport node . how many ever leaf-node are present that many times the data is encrypted. By reducing the eligible children in access tree the transport node is reduced. The rule of access tree is like the transport path is simplified and remaining node are erased so that there is less computational time

SCHEME DISCUSSION

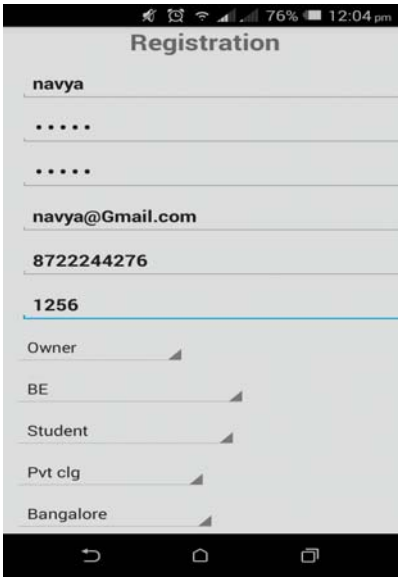
Computational cost on data owner: the hierarchy layered moddl of the access tree structures gives us with multiple levels of file sharing all these files are encrypted using one integrated access tree structure from this data owner can encrypt different level and generate integrated ciphertext only by executing the AES algorithm once common attributes may appear in the tree structure it should appear once.the computational cost is reduced ,therefore encryption efficiency is improved by data owner.

Computational cost on user: the decryption process ,all the user who are given authorization to decrypt the files with the help of secret key since transport nodes are added in access structure with k different level nodes and bilinear operation of common nodes is used in access of file when only common node is seen one time decryption cost is reduced by 2n(m-1/m) if user need to decrypt the files.

MODULES

1.Registration and Login

- This module is authentication module.
- User enters his/her details by filling up the registration form.
- Successfully registered user can login using his/her user name and password.
- User's details are stored to the database and verified.



2.Key Generation

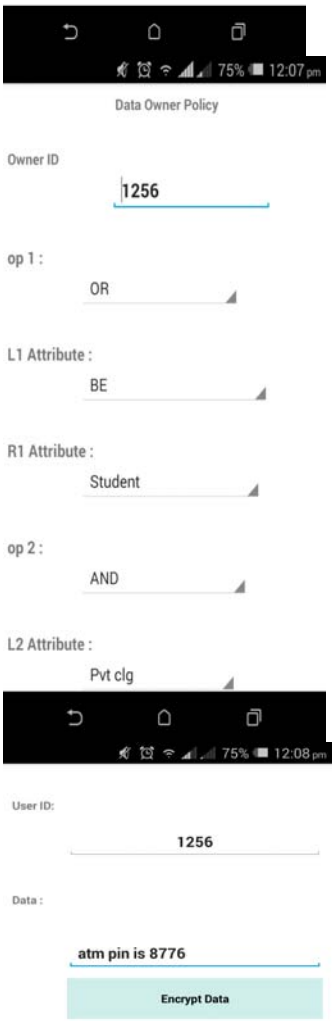
- This module runs from authority side.
- Authority make a set up using security parameter, then using Master key and Public key, Authority generates a secret key for user.

Server Configuration Module

- We are using Tomcat7 as a web server.
- server collect all request from mobile user side and process.
- After processing request it will sent a response to mobile user.

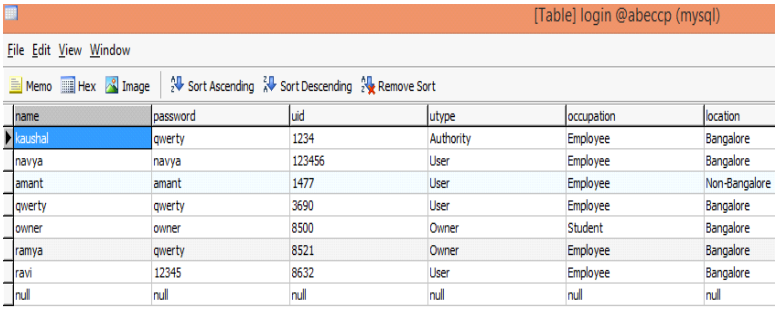
Access Tree Structure Policy Creation

- Before upload data on server user create a access policy tree structure using operators(OR and AND)and attributes.
- Before data encryption data owner has to create policy.
- Policy creation is a multi-level binary search tree where leaf nodes contain attributes and rest of nodes having operators.



3.Data Upload to Server

- After creating a policy we have to encrypt our data using AES symmetric algorithm.
- AES is a symmetric i.e., only one key will generate to encrypt and decrypt both.
- Data owner upload the file after data encryption using attributes.



name	password	uid	utype	occupation	location
kaushal	qwerty	1234	Authority	Employee	Bangalore
navya	navya	123456	User	Employee	Bangalore
amant	amant	1477	User	Employee	Non-Bangalore
qwerty	qwerty	3690	User	Employee	Bangalore
owner	owner	8500	Owner	Student	Bangalore
ramya	qwerty	8521	Owner	Employee	Bangalore
ravi	12345	8632	User	Employee	Bangalore
null	null	null	null	null	null

4.Data Decryption by End User

- Decryption is done by end user.
- After uploading data on to the server,the user need to satisfy all the attributes of the owner.
- If the attributes satisfy then the data will be decrypted.

In this paper,we proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing.The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files.Therefore,both ciphertext storage and time cost of encryption are saved.

Conclusion

The adequacy of sharing the progressive documents in distributed computing is made reliant on our Proposed framework CP-ABE. The credits identified with that ciphertext segment various leveled records are encoded with an incorporated get to structure and the figure content segments identified with characteristics could be shared by the documents. Henceforth, both figure content stockpiling and time cost of encryption is spared. The proposed plot has favorable position that clients can decode all approval documents by processing mystery key once.

In this manner, the time cost of unscrambling is additionally spared if the client needs to decode various documents. Besides, the proposed plan is turned out to be secure under DBDH suspicion. The proposed framework gives better client experience to culinary related issues for clients carrying on with a period obliged way of life. The client enters the accessible basic supplies or the accessible utensils or the accessible time as contribution to the application into the channels.

References

[1] Tao Jiang , Xiaofeng Chen , Jin Li , Duncan S. Wong , Jianfeng Ma. In 2010 IEEE 3rd Int.Conf. Cloud Comput. IEEE. doi:10.1109/CLOUD.2010.58.

[2] Kaitai Liang , Joseph K. Liu , Duncan S. Wong , Willy Susilo, in Proc. IEEE Grid Comput. Environ. Workshop, 2008, pp. 1–10.

[3] Tsz Hon Yuen , Ye Zhang , Siu Ming Yiu , and Joseph K. Liu, in Proc. 4th Adv. Int. Conf. Telecommun., 2008, pp. 13–18.

[4] Kaitai Liang, Man Ho Au, in Thomas j. Watson Research Center, Rc23980 in 2006.

[5] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo ,Future Gener. Computer .Syst. ,vol. 28 ,no .2 ,pp.358–367 ,201

Author's Details

1.Ramya B Student, computer science, T.John Institute of Technology, Karnataka, India, Ramya55388@gmail.com.

2.Naya N.P, Student, computer science, T.John Institute of Technology, Karnataka, India, Navyavijay26@gmail.com

3Swetha V.S Student, computer science, T.John Institute of Technology, Karnataka, India, swetha26.06@gmail.com

4Tejaswini J Student, computer science, T.John Institute of Technology, Karnataka, India, tejashwinijayaram9665@gmail.com