# A Circuit Hybrid Attribute Based Encryption of Data with Fragmentation for Increasing Ideal Performance and Security in Cloud Computing

**Roma J. Ahuja [1], Kalyani B. Hailkar[2], Saurabh V. Kale[3], Prof A.A.Khatri[4]**
[1, 2, 3, 4] Dept of Computer Engineering
[1, 2, 3, 4] Jaihind College of Engineering, Pune.

***Abstract***- *Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing offers the number of significant advantages. One of the main advantage of cloud computing is pay-as-per-use, which means according to the use of service the customer has to pay. Where the prime disadvantage of cloud computing is achieving security to the data which is store in cloud. The data compromise may occur due to attacks by other users and node within cloud. In this paper, We propose Hd-ABE (Hybrid Attribute Based Encryption ) In which data owner should set the access structure of attributes with encrypted data , The user only whose attributes are match with access structure of owner only that user can decrypt the data. To secure data which is supposed to be stored within a single node have been replaced by DROPS (Division and Replication of Data in the cloud for Optimal Performance and Security) methodology, in which we divide the file into fragments, and replicate the fragmented data over the cloud.*

***Keywords***- Cloud computing, Security, Hybrid attribute based encryption, Fragmentation.

## I. INTRODUCTION

Cloud computing is a technique which describes the combination of different data, software which are accessible via internet. Cloud computing is innovation that uses advanced computational power and improved storage capabilities. In this cloud computing prime disadvantage is security of data, to provide end-to-end data security and privacy in the cloud, sensitive data has to be encrypt before outsourcing to protect data privacy.

In cloud computing, effective data utilization is very difficult task because data may hack by other users and node within cloud .As application move to cloud computing platform, A hybrid attribute based encryption in which every cipher text is label with some attributes along with location and a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instance is in the allowed time interval and attributes associated with ciphertext satisfy the key's access structure.

Consider the example like health care organizations store data files in the cloud by using CP-ABE and L-ABE under certain access policies. in this system doctor encrypt the data with access structure of attributes and location attribute , the patient who's attributes are match with access structure only that patient can decrypt or download the data , It provide multiple parallel efforts underway to modernize medical record system for greater efficiency , improved patient care, patient safety and cost saving.

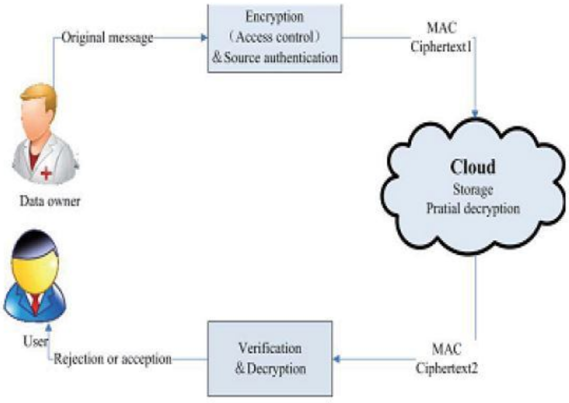


Fig. Medical data sharing system

To increase more security in cloud data which is store in single node we can use DDROPS (Division and Replication of Data in the cloud for Optimal Performance and Security) methodology, in which we divide the file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

## II. LITERATURE SURVEY

*Research Paper 1*

1. *Title*: Identity Based Cryptosystem and signification scheme
2. *Authors*: Adi Shamir
3. *Description:*

IDE is nothing but Identity based encryption. Original IDE gives by Adi Shamir in [1]1984. In Identity based encryption view the identities as a string of characters. Identity based encryption (IDE), is an important primitive of ID_based cryptography. As such it is a type of public key encryption in which the public key of user is some unique information about the identity of the user for example a user's email address, if owner of data want to send same message or same data to multiple user at a time then it is necessary to select email ID of all users. So it is a time consuming process and not so secure.

*Research Paper 2*

1. *Title*: Fuzzy Identity Based encryption

2. *Authors*: Sahai and Waters

3. *Description*:

Fuzzy identity based was introduced by sahai and waters in 2005. They modify original IDE given by Adi Shamir in [1]1984.In fuzzy identity based encryption view the identities as a set of attribute; It is also called as Attribute Based Encryption. Fuzzy IBE is first paper give the concept of attribute based encryption with public key cryptography. Fuzzy IBE is an attribute type encryption where set of attributes are used to represent an identity. The set of attribute are set by owner when owner wants to send one data to multiple users, the users whose attributes get matched with specified attribute, will only get the access to the data. The disadvantage of Fuzzy IBE is data owner need to use every authorized user's public key.

*Research Paper 3*

1. *Title*: Key-Policy Attribute Based Encryption (KP-ABE).

2. *Authors*: Parmar Vipul Kumar & Rajanikanth Aluvalu

3. *Description:*

KP-ABE (Key-Policy Attribute Based Encryption)is modified form of classical model of ABE. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. [3, 4] Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In a Key-policy attribute based encryption system, Cipher text are branched by the sender with the set of descriptive attributes. The disadvantages of KP-ABE are like Encryptor can not decide who can decrypt the encrypted data, it can only choose descriptive attributes for the data, and has no choice but to trust the key issuers.

*Research Paper 4*

1. *Title*: Cipher text-Policy Attribute Based Encryption An Expressive, Efficiently and provably secure Realization.

2. *Authors*: Brent Wate

3. *Description:*

CP-ABE is modified form of classical model of ABE, It fulfill some drawbacks of KP-ABE. In CP-ABE encryptor can decide who can decrypt the encrypted data. In CP-ABE, each user is linked with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP-ABE technique, encrypted data can be kept confidential and secure against collusion attacks. The disadvantage is in CP-ABE only static attribute are specified there is no dynamic attribute is used.

*Research Paper 5*

1. *Title*: Designing a Hybrid attribute-Based encryption scheme supporting Dynamic Attribute.

2. *Authors*: Stefan G.Weber

3. *Description:*

Hybrid attribute based encryption is attributes based, as it allows encryption under logical combination of attributes i.e. properties that users satisfy. It is hybrid; as it combines Ciphertext attribute based encryption (CP-ABE) [5] with location based encryption (LBE) on the level of symmetric key. It handle both static and dynamic attribute like location.The location based encryption is used for security mobile communication by limiting area inside which the recipient can decrypt the message.

*Research Paper 6*

1. *Title*: SECURE DYNAMIC FRAGMENT AND REPLICA ALLOCATION IN CLOUD STORAGE

2. *Authors*: P. Anand , R.Bharath, C.Ganapathy, S. Sam Victor.

3. *Description:*

In this paper we get information about hoe the data is fragment and store in different nodes in cloud. This is used to increasing security of data which is store in cloud. For achieving this security DROP Methodology is used. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data

File that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

## III. MOTIVATION

Tampering:- Tampering of sensitive data by buisness opponent for profit reasons otherwise business rankings. Tampering here means manipulating the data, making changes to the originally stored data .This action is performed by business opponents or hackers for profit reason, ranking, emotional or mental harassment.

Data stored in a single node:-In this the data is stored in cloud, but on a single node. If successful attack takes place on that node the whole data gets hacked.

Insecure key management system:-In cloud computing the data is stored in cloud. And the key required to decrypt the ciphertext data is also provided by the cloud. If the key gets hacked by the hacker the entire data gets in control of the hacker.

## IV. OBJECTIVE

1. *Data Security:* -

Providing security to data by using a strong encryption algorithm which is difficult to break. The prime disadvantage of cloud computing is achieving security to the data which is stored in cloud. To achieve this we are using AES algorithm which will be very helpful in achieving the respected output i.e. data security.

2. *Data Confidentiality:* -

We can see now a day’s data confidentiality is a very serious issue. Data theft is harming in business, medical, and various IT sectors. Different hackers use various techniques to hack the confidential data, so as to achieve own personal profits or some personal benefits. Data theft can be at any level, or for different reasons eg:- in IT sectors administrator and office employees have access to different data or copyrights of the company. All the data is stored in companies database server, desktop computers or sometimes handheld devices like memory stick, hard drives etc. The access is given to the employees because they work for the company. But employees make misuse or manipulate the data. Reason can be anything like if employee is suppose to resign the job, or if the employee is terminated from the company, or if any other competitive company has provided the employee with economical benefit for providing the confidential data which can give other companies economical profit. So our system is aiming to provide system which will give strong data confidentiality. We are making use of hybrid attribute based encryption in our system. Hybrid here means combination of CP-ABE with Location Based Encryption (LBE) on the level of symmetric key. It will handle both static and dynamic attribute like location. The LBE is used for secure mobile communication by limiting area inside which the recipient can decrypt the message.

3. *Data Fragmentation:* -

For security of data stored in cloud we will be using DROP methodology. In this methodology, we divide a file in fragments and replicate the fragmented data over the cloud nodes. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

## V. SYSTEM ARCHITECTURE

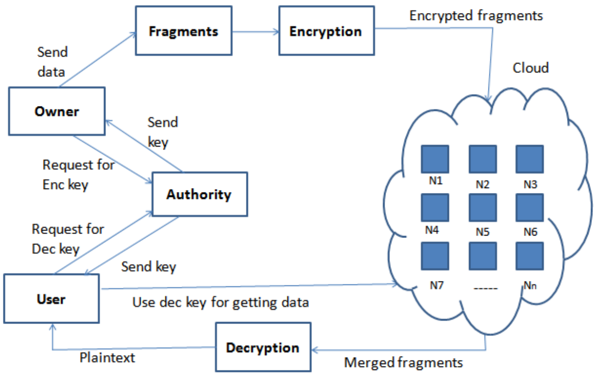


Fig .Proposed system

The proposed system design circuit ciphertext-policy attribute-based encryption with time-specified attributes scheme has been developed. In this scheme, every ciphertext is labeled with some attribute and a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure.

The system contains four modules,

1) Owner
2) User
3) Authority
4) Cloud Server

- Owner: Owner is responsible to upload the data in numbers of fragments and assign the attribute to data and create the access structure.
- Authority: Authority is responsible to perform authentication of owner and user as well as to send keys, for encryption and decryption to owner and user respectively if they are valid.
- User: User is responsible to access or download the data which is given by owner.
- Cloud Server: Cloud server is responsible to provide storage space to store the data into different nodes and partially decrypt the data when user wants to access.

*Advantages:*

- Achieve access control and keep data confidential.
- Reduce the computing cost.
- Achieves security by dividing the data into multiple fragments and stores on multiple node

## VI . WORKING

When owner wants to store data on cloud he has to get permission from authority to do this. For this owner has to made request to authority for encryption key. Authority verifies whether the requested party is trustable or not. If so, then encryption key is getting provided to that specific owner. By using encryption key data is send by owner.

In the proposed system, for achieving high security we are using concepts of fragmentation. In this before storing data in cloud, that particular data is get fragmented and after this fragmented data get encrypted and stored in cloud on multiple node randomly.

When any user wants that specific data he has to make request to authority for decryption key. For this authority has to verify whether requested user is trustable or not. If the user is eligible, authority provides decryption key and user can easily get decrypted data. For this data which Is stored on multiple nodes in the form of fragments, firstly merged together and after that user gets data in plaintext.

## VII. METHEDOLOGIES

The proposed model which is developed does not only depend on the system's working process, but also it depends on the working of the flow of the process which needs to be considered. The proposed model acts as the platform for the users to address the problem regarding any issue and which should be handled carefully. The proposed system design circuit cipher text-policy attribute-based encryption with time-specified attributes scheme has been developed .In this scheme, every cipher ext is labeled with some attribute and a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. To achieve the more security, the data is divided into multiple fragments and store on multiple nodes instead of storing on single node. This system is mixed with verifiable computation the data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time.

*Algorithm and Technique:*

1. AES Algorithm: - 128bit AES algorithm for Encryption.

2. Fragmentation Algorithm : -

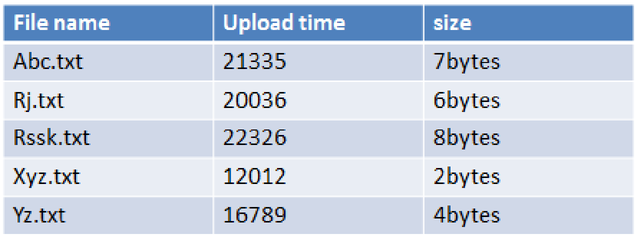
```
Input: File.
Output: Chunks.
Algorithm:
step 1. If file is to be split go to step 2 else go to step 8
step 2. Input source path, destination path
step 3. Size = size of source file
step 4. Fs = Fragment Size
step 5. NoF = number of fragments
step 6. Fs = Size/Nof
step 7. We get fragments
step 8. End
```

3. T-coloring Algorithm:

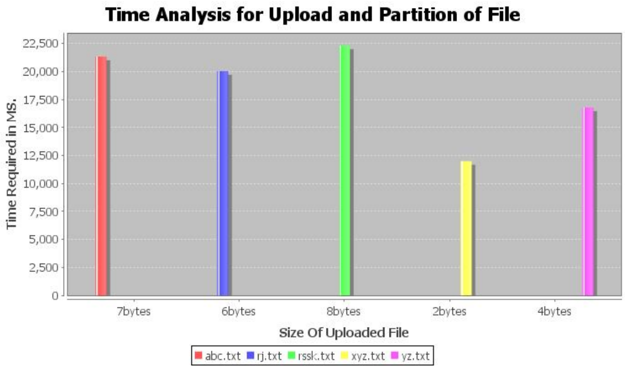
```
Input: No.of fragmented data.
Output: Randomly placed fragments in different nodes.
Algorithm:
O = {O1, O2…On}
o = {size of (O1) , size of (O2) … size of (On)}
col = { open color; close color}
cen = {cen1,cen2,…cenM}
col open color i
cen ceni i
Compute :
f or each Ok > O do
select Si S Si index of (max(ceni))
if colSi = open color and si >= ok then
Si ←Ok
si ←si - ok
colSi ←close color
Si ←distance(Si;T)P
colSi ←close color
end  if
end  for
```

## VIII. PERFORMANCE ANALYSIS

In order to evaluate the performance of our system “a circuit HB-ABE of data with fragmentation to improve the ideal performance and security in cloud computing”  we have tested our system by implementing time analysis chart which clearly shows how much time is taken by the system for completing the upload and fragmentation of a file in cloud and we have got some results out of it which tells that the time required for the upload and partition of file is directly proportional to the size of the uploaded file and it also depends on the network speed of the user PC.



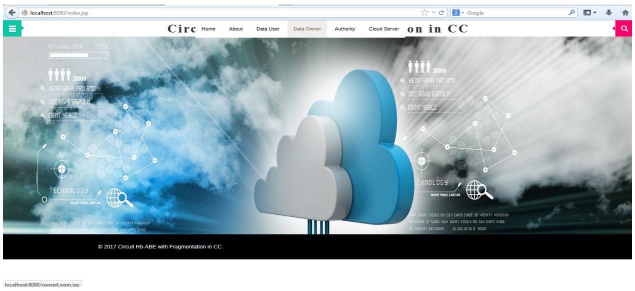
| File name | Upload time | size |
|---|---|---|
| Abc.txt | 21335 | 7bytes |
| Rj.txt | 20036 | 6bytes |
| Rssk.txt | 22326 | 8bytes |
| Xyz.txt | 12012 | 2bytes |
| Yz.txt | 16789 | 4bytes |



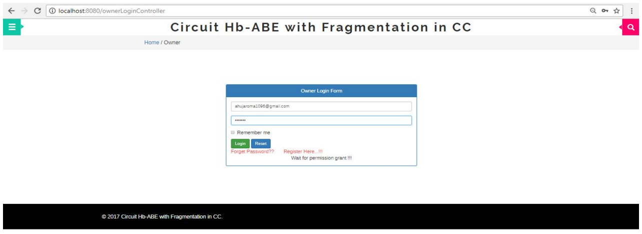
## IX. RESULTS

Screenshots:-

This is index page from which data owner in open



This is owner login page and it is waiting for TPA authorization


localhost:8080/ownerLoginController
Circuit Hb-ABE with Fragmentation in CC
Home / Owner
Login
Reset
Forget Password??
Register Here...!!!
© 2017 Circuit Hb-ABE with Fragmentation in CC.

Owner Login Form

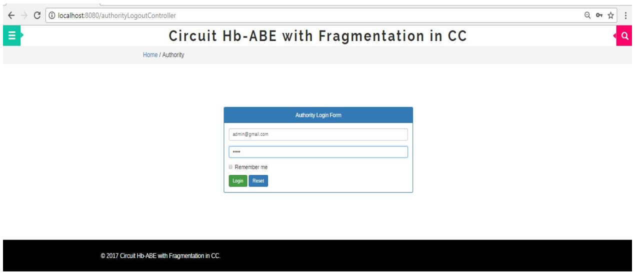
ahujaroma1096@gmail.com

•••••••

□ Remember me

Wait for permission grant !!!

This is authority login page



localhost:8080/authorityLogoutController

Circuit Hb-ABE with Fragmentation in CC

Home / Authority

Authority Login Form

admin@gmail.com

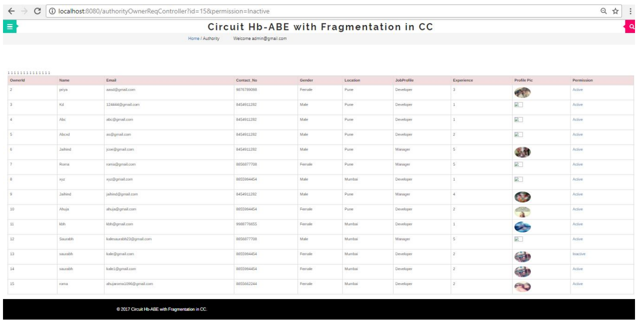
•••••

□ Remember me

Login Reset

© 2017 Circuit Hb-ABE with Fragmentation in CC.

This is Permission grant page where TPA actives the valid person.



localhost:8080/authorityOwnerReqController?id=15&permission=Inactive

Circuit Hb-ABE with Fragmentation in CC

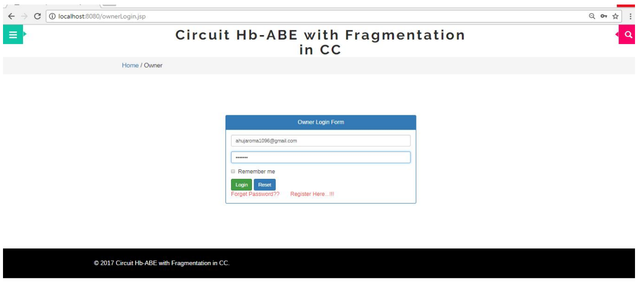
Home / Authority Welcome admin@gmail.com

1 1 1 1 1 1 1 1 1 1 1 1 1 1

| OwnerId | Name | Email | Contact_No | Gender | Location | JobProfile | Experience | Profile Pic | Permission |
|---|---|---|---|---|---|---|---|---|---|
| 2 | priya | aasd@gmail.com | 9876789098 | Female | Pune | Developer | 3 | | Active |
| 3 | Kd | 124444@gmail.com | 8454911282 | Male | Pune | Developer | 1 | | Active |
| 4 | Abc | abc@gmail.com | 8454911282 | Male | Pune | Developer | 1 | | Active |
| 5 | Abcxd | as@gmail.com | 8454911282 | Male | Pune | Developer | 2 | | Active |
| 6 | Jaihind | jcoe@gmail.com | 8454911282 | Male | Pune | Manager | 5 | | Active |
| 7 | Roma | roma@gmail.com | 8856877708 | Female | Pune | Manager | 5 | | Active |
| 8 | xyz | xyz@gmail.com | 8855994454 | Male | Mumbai | Developer | 1 | | Active |
| 9 | Jaihind | jaihind@gmail.com | 8454911282 | Male | Pune | Manager | 4 | | Active |
| 10 | Ahuja | ahuja@gmail.com | 8855994454 | Female | Pune | Developer | 2 | | Active |
| 11 | kbh | kbh@gmail.com | 9988776655 | Female | Mumbai | Developer | 1 | | Active |
| 12 | Saurabh | kalesaurabh23@gmail.com | 8856877708 | Male | Mumbai | Manager | 5 | | Active |
| 13 | saurabh | kale@gmail.com | 8855994454 | Female | Mumbai | Developer | 2 | | Inactive |
| 14 | saurabh | kale1@gmail.com | 8855994454 | Female | Mumbai | Developer | 2 | | Active |
| 15 | roma | ahujaroma1096@gmail.com | 8855662244 | Female | Mumbai | Developer | 2 | | Active |

© 2017 Circuit Hb-ABE with Fragmentation in CC.

Now owner is active and ready to login.



localhost:8080/ownerLogin.jsp

Circuit Hb-ABE with Fragmentation in CC

Home / Owner

Owner Login Form

ahujaroma1096@gmail.com

•••••••

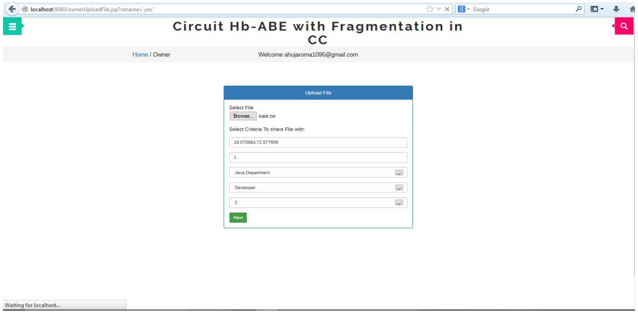
□ Remember me

Login Reset

Forget Password?? Register Here...!!!

© 2017 Circuit Hb-ABE with Fragmentation in CC.

This is file upload page on owner side.



localhost:8080/ownerUploadFile.jsp?rename='yes'

Circuit Hb-ABE with Fragmentation in CC

Home / Owner Welcome ahujaroma1096@gmail.com

Upload File

Select File

Browse... kale.txt

Select Criteria To share File with:

19.075984,72.877656

1

Java Department

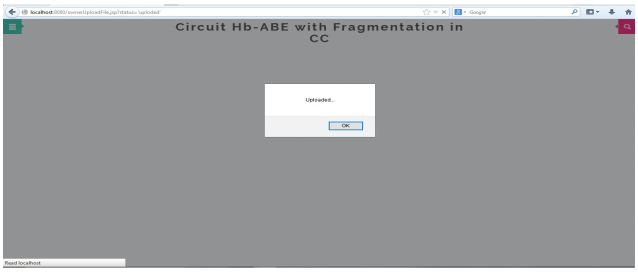
Developer

2

Next

Waiting for localhost...

File is uploaded by specifying user attributes.



localhost:8080/ownerUploadFile.jsp?status='uploded'

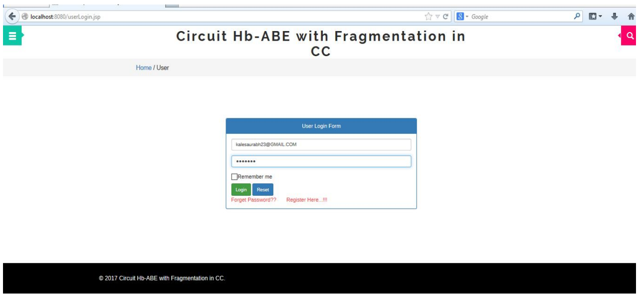
Circuit Hb-ABE with Fragmentation in CC

Uploaded...

OK

Read localhost

This is user login page.



localhost:8080/userLogin.jsp

Circuit Hb-ABE with Fragmentation in CC

Home / User

User Login Form

kalesaurabh23@GMAIL.COM

•••••••

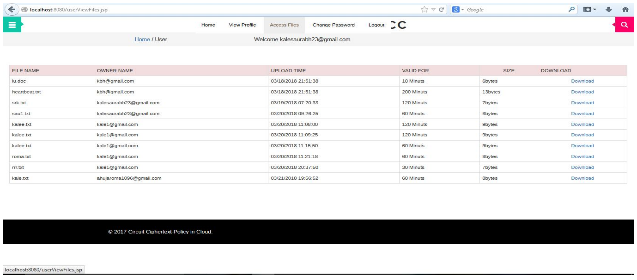
□ Remember me

Login Reset

Forget Password?? Register Here...!!!

© 2017 Circuit Hb-ABE with Fragmentation in CC.

These are the available files to be downloaded on the user side.



localhost:8080/userViewFiles.jsp

Home View Profile Access Files Change Password Logout CC

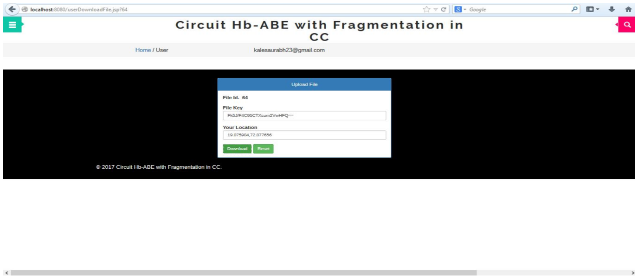
Home / User Welcome kalesaurabh23@gmail.com

| FILE NAME | OWNER NAME | UPLOAD TIME | VALID FOR | SIZE | DOWNLOAD |
|---|---|---|---|---|---|
| iu.doc | kbh@gmail.com | 03/18/2018 21:51:38 | 10 Minuts | 6bytes | Download |
| heartbeat.txt | kbh@gmail.com | 03/18/2018 21:51:38 | 200 Minuts | 13bytes | Download |
| srk.txt | kalesaurabh23@gmail.com | 03/19/2018 07:20:33 | 120 Minuts | 7bytes | Download |
| sau1.txt | kalesaurabh23@gmail.com | 03/20/2018 09:26:25 | 60 Minuts | 8bytes | Download |
| kalee.txt | kale1@gmail.com | 03/20/2018 11:08:00 | 120 Minuts | 9bytes | Download |
| kalee.txt | kale1@gmail.com | 03/20/2018 11:09:25 | 120 Minuts | 9bytes | Download |
| kalee.txt | kale1@gmail.com | 03/20/2018 11:15:50 | 60 Minuts | 9bytes | Download |
| roma.txt | kale1@gmail.com | 03/20/2018 11:21:18 | 60 Minuts | 8bytes | Download |
| rrr.txt | kale1@gmail.com | 03/20/2018 20:37:50 | 30 Minuts | 7bytes | Download |
| kale.txt | ahujaroma1096@gmail.com | 03/21/2018 19:56:52 | 60 Minuts | 8bytes | Download |

© 2017 Circuit Ciphertext-Policy in Cloud.

localhost:8080/userViewFiles.jsp

Fill the empty fields by the user, if user is a valid user file is downloaded.



localhost:8080/userDownloadFile.jsp?64

Circuit Hb-ABE with Fragmentation in CC

Home / User kalesaurabh23@gmail.com

Upload File

File Id. 64

File Key

Fk5J/F4C95CTXsum2VwHFQ==

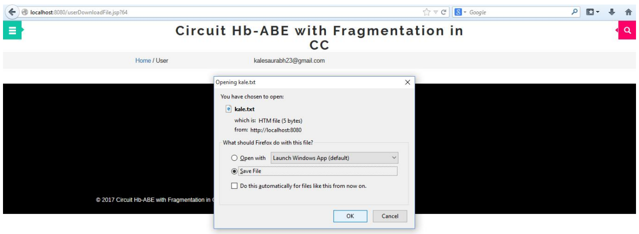
Your Location

19.075984,72.877656

Download Reset

© 2017 Circuit Hb-ABE with Fragmentation in CC.

If valid information is entered file is ready to be download.



localhost:8080/userDownloadFile.jsp?64

Circuit Hb-ABE with Fragmentation in CC

Home / User kalesaurabh23@gmail.com

Opening kale.txt

You have chosen to open:

kale.txt

which is: HTM file (5 bytes)

from: http://localhost:8080

What should Firefox do with this file?

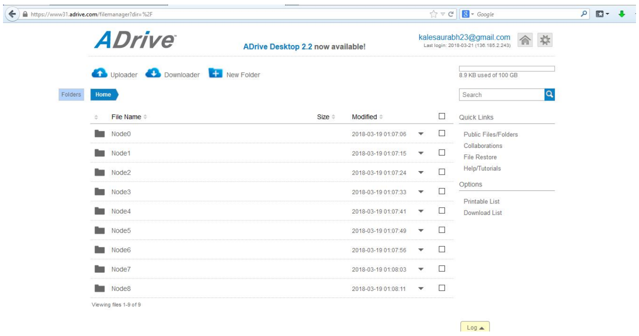
○ Open with Launch Windows App (default)

● Save File

□ Do this automatically for files like this from now on.

© 2017 Circuit Hb-ABE with Fragmentation in C

This is the cloud framework where 9 nodes are available.



https://www31.adrive.com/filemanager?dir=%2F

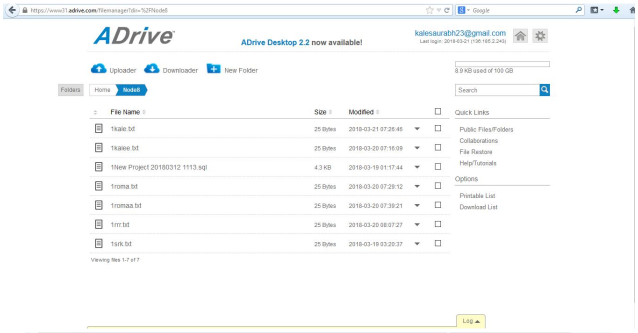
kalesaurabh23@gmail.com
Last login: 2018-03-21 (136.185.2.243)

8.9 KB used of 100 GB

| File Name | Size | Modified |
|---|---|---|
| Node0 | | 2018-03-19 01:07:06 |
| Node1 | | 2018-03-19 01:07:15 |
| Node2 | | 2018-03-19 01:07:24 |
| Node3 | | 2018-03-19 01:07:33 |
| Node4 | | 2018-03-19 01:07:41 |
| Node5 | | 2018-03-19 01:07:49 |
| Node6 | | 2018-03-19 01:07:56 |
| Node7 | | 2018-03-19 01:08:03 |
| Node8 | | 2018-03-19 01:08:11 |

Viewing files 1-9 of 9

The fragmented files are stored on node 5 and node 8.



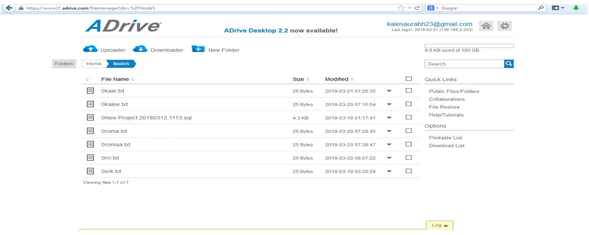
https://www31.adrive.com/filemanager?dir=%2FNode8

kalesaurabh23@gmail.com
Last login: 2018-03-21 (136.185.2.243)

8.9 KB used of 100 GB

| File Name | Size | Modified |
|---|---|---|
| 1kale.txt | 25 Bytes | 2018-03-21 07:26:46 |
| 1kalee.txt | 25 Bytes | 2018-03-20 07:16:09 |
| 1New Project 20180312 1113.sql | 4.3 KB | 2018-03-19 01:17:44 |
| 1roma.txt | 25 Bytes | 2018-03-20 07:29:12 |
| 1romaa.txt | 25 Bytes | 2018-03-20 07:39:21 |
| 1rrr.txt | 25 Bytes | 2018-03-20 08:07:27 |
| 1srk.txt | 25 Bytes | 2018-03-19 03:20:37 |

Viewing files 1-7 of 7



https://www31.adrive.com/filemanager?dir=%2FNode5

kalesaurabh23@gmail.com
Last login: 2018-03-21 (136.185.2.243)

8.9 KB used of 100 GB

| File Name | Size | Modified |
|---|---|---|
| 0kale.txt | 25 Bytes | 2018-03-21 07:26:35 |
| 0kalee.txt | 25 Bytes | 2018-03-20 07:15:54 |
| 0New Project 20180312 1113.sql | 4.3 KB | 2018-03-19 01:17:41 |
| 0roma.txt | 25 Bytes | 2018-03-20 07:28:45 |
| 0romaa.txt | 25 Bytes | 2018-03-20 07:38:47 |
| 0rrr.txt | 25 Bytes | 2018-03-20 08:07:22 |
| 0srk.txt | 25 Bytes | 2018-03-19 03:20:29 |

Viewing files 1-7 of 7

## X . FUTURE WORK

Until now we have successfully fragmented .txt files, now our next approach will be heading towards fragmentation of png , jpeg files and successfully storing on to the cloud. We can also implement more modern algorithm for encryption and decryption of data. In future we can also think on fragmenting Audio (mp3), Video (mp4, hd, 3gp, etc.) files and storing on to the cloud in encrypted format.

## XI. CONCLUSION

The Circuit Hb-ABE is the methodology which is applied on secret data, so as to convert it in to confusing, tough, and difficult to break cipher text data and this data is further passed through DROPS methodology, a cloud storage security scheme that focuses on two important points, first is security and another is retrieval time. Here the cipher text data which is produced is fragmented into parts and deployed on multiple nodes. T-coloring algorithm is the technique which has been implemented in our project which allows us to deploy fragments on different nodes. The overall methodology makes it very difficult for the attacker to access the data even if it has made a successful attack. No node will allow deployment of more than one fragment of the same file. The implementation of DROPS found very advantageous. The results of the simulations revealed that the simultaneous focus on the security and performance resulted in increased security level of data accompanied by a slight performance drop.

## REFERENCES

[1] Adi Shamir ,"Identity Based Cryptosystem and signification schemes".

[2] A. Sahai and B. Waters, "Fuzzy identity based encryption", Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn, pp. 457-473, 2005

[3] N.krishna L.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 – Oct 2013.

[4] Parmar Vipul Kumar, Rajanikanth Aluvalu" Key-Policy Attribute Based Encryption(KP-ABE)",International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 2, 2015.

[5] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptograph. Conf. Public Key Cryptograph, 2011.

[6] Stefan G.Weber," Designing a Hybrid attribute-Based encryption scheme supporting Dynamic Attribute",in Proc. 27th Int. Cryptol.Conf.,2016

[7] P.Anand, R.Bharath, C.Ganapathy, S. Sam Victor,"SECURE DYNAMIC FRAGMENT AND REPLICA ALLOCATION IN CLOUD STORAGE", International Journal of Computer Informatics & Technological Engineering Volume (3) Issue (3) March 2016