IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Improving privacy and Authentication in Decentralizing Multi Authority attribute based Encryption in cloud Computing

NALLAPARAJU JNANA DURGA BHAVANI [#1], L. SOWJANYA [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

Till now almost all the cloud data which is collected from remote locations is stored in the centralized storage medium, there are a lot of security issues that takes place in the centralized data storage. It is facing with a lot of problems like no proper data authentication and data authorization present in the networks. Hence we try to utilize the new principle known as data de-centralization in which the storage and access permission will lie in the individual departments rather than in the cloud server. In this proposed paper we try to use a third party global identifier in order to verify the key permissions which is granted by the data owner and this will be generating the keys for the data users who try to request the data. In this proposed thesis we try to develop a new scheme by adding a global identifier like Attribute Authority (AA) for providing access keys for the data users who wish to access the sensitive information from the cloud server. In this proposed work we try to construct Composite Order Bilinear Groups scheme for providing access facility for the data users and provide more security for the sensitive data. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is very efficient to access the data in a de-centralized manner by using a global identifier.

Keywords

Cloud Computing, Composite Order Bilinear Groups**,** De-centralization, Data Authentication, Attribute Authority

1. INTRODUCTION

Cloud computing enabled a lot of web users to store their sensitive data into un-trusted cloud server to achieve the scalable services on-demand. There are lot of security requirements which arise in the current days in order to store and access the information in a secure manner. For this we need to use a strong encryption technique to provide security for the data storage and management in cloud computing[1]. In current days almost all the cloud servers try to use normal cryptography techniques for providing security for their sensitive data which is stored and accessed from the remote locations. They are not completely providing security for the data which is stored in their centralized location. Hence in this current paper we mainly discuss about the importance and advantages of using attribute-based encryption (ABE) for storing and accessing the information in a secure manner in cloud computing. As we all know that lot of small scale and large scale companies try to share their confidential data on the cloud servers, and they want to share access preference for only some rather than for all. Hence this ABE algorithm is best in providing data access for the individuals who want to share and access the information in a confidential manner[2].

In general the primitive ABE algorithm can share security for only one domain or organization at a time and in reality this is not giving enough solution for the end users who wish to store and access the information from the cloud server. For example if we take an example of RTO works such as drivers' licenses and registration information is mainly operated by the RTO department with several sub departments[3]. One Authority cannot grant all the permissions for the end users and this should be monitored and granted by several individual departments which are used for key generations from remote locations. Therefore, primitive ABE cannot meet distribution demands of the end users who try to access and store the information in a secure manner. Hence we try to organize the new mode of security primitive like decentralized multi-authority ABE in which the data access can be monitored and operated by several authorities who are present in the remote locations. The authorities may be differ from one level to another level in terms of accessing and sharing the permissions under various key distributions cannot be undertaken by the same attribute authority. Moreover, access strategies may be distributed based on attributes of different authorities[4].

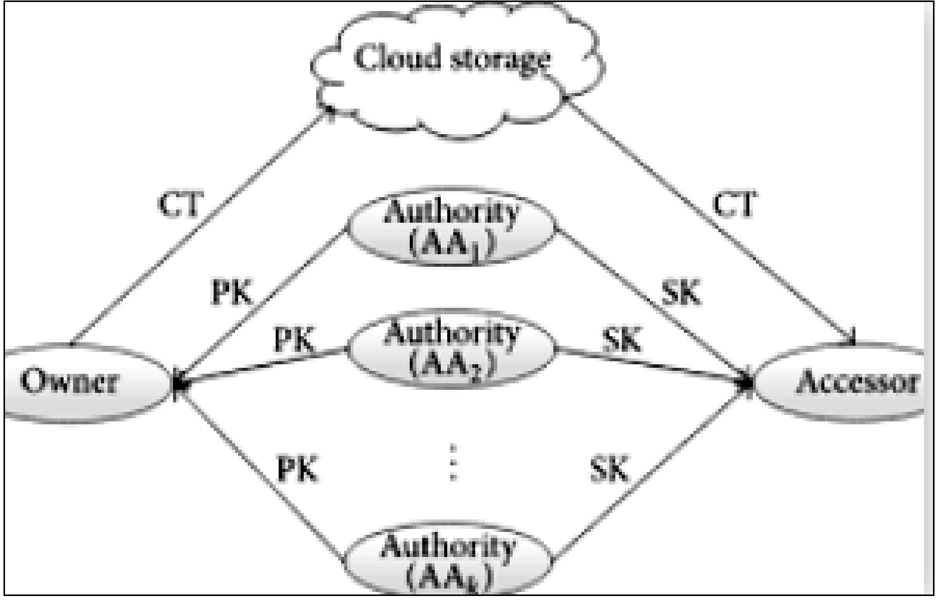


Figure. 1. Represents the Working of Multi Authority ABE Algorithm

Single-authority ABE algorithm mainly depends on random private keys which are generated with users' private keys and decryption is performed by reconstructing the secret values. In Single-authority attribute based encryption[5], each user is given with set of attributes and share a random key for storing the data in order to avoid collusion attacks. In this present paper we try to design decentralizing multi-authority ABE, where the private keys which are generated by different authorities do not communicate with one another and once if any user try who wish to access the key ,he need to get the access from the global identifier and then only the data can be accessed in plain text manner[6].

From the figure 1, we can clearly identify a multi authority ABE algorithm contains multiple global identifiers which are used for giving permissions for the files which are uploaded by the data owner. Here the data which is to be uploaded into the cloud server is converted into cipher text and the data will be then uploaded into the centralized storage medium[7]. Now if the data user who want to access the file need to send file access request to this multi key authority then only the data can be accessed by the end users. If the multi key authority doesn't grant the permissions for the user request the data will not be granted to access in plaintext manner. If the user who receives the permission from multi authority can only access the file in a plain text manner.

2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

MOTIVATION

Two well-known authors, M. H. Au and A. Kapadia [6] have written a paper on “Practical reputation-based blacklisting without TTPS”. In this paper the authors concentrated about the preventing of some anonymous credential schemes which revoke access for misbehaving users. The authors try to propose a novel scheme like BLACR, which support the reputation-based and they try to make the access denied. The major drawback of BLACR is linear combination of data along with the size of reputation lists.Here we tried to proposed a revocation based storage scheme in which the if any revoked users is identified thus will immediately mark such user as black list and this will not utilize the services from that black list user.

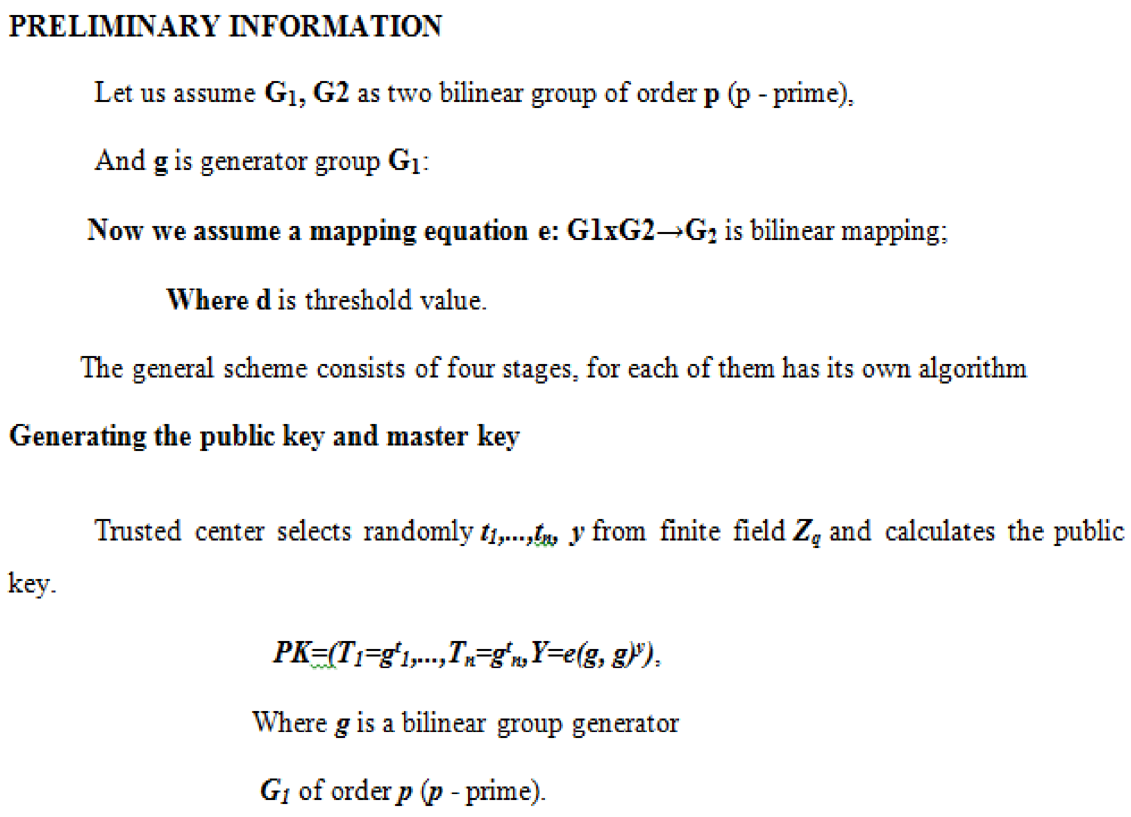
Two well-known authors, M. H. Au, W. Susilo, and Y. Mu [7] have written a paper on ” Constant-size dynamic *k*-TAA”. In this paper the authors concentrated more about (k-TAA) schemes which allow a group of members to authenticated anonymously by the set of application providers for some time period.Here the authors mainly concentrated more on the principle of data revocation and also they greatly identify the similarity between normal user and revoked user under the own group. In this paper, the authors try to construct a dynamic k-TAA scheme with very less time and space complexity and it is achieved for less key size. The authors mainly deal with the zero-knowledge protocol using some random oracle model under Diffie–Hellman inversion assumption.

Two well-known authors D. Song and D. Wagner[8], has written a paper on “Practical techniques for searches on encrypted data”. In this paper the authors mainly concentrated about the security and privacy risks and how to reduce these risks on data storage servers such as mail servers and file servers[8]-[10]. They said that one need to sacrifice functionality of their server usage for security. For example, if a client who wishes to retrieve the documents based on search keyword, he needs to know the circumstances about that file and about the confidentiality. Here we try to define the cryptography function for enabling the security primitive and also we try to provide a proof of security to achieve the challenges faced by the cloud computing.

3. THE PROPOSED COMPOSITE ORDER BILINEAR GROUPS SCHEME

In this section we try to discuss about the proposed method which uses the Bilinear group scheme for sharing the data under centralized manner[11] by using the facility of global identifier. Here the term global identifier is used for providing key access and security for the end users data[12].

PRELIMINARY INFORMATION



PRELIMINARY INFORMATION

Let us assume $\mathbf{G_1}$, **G2** as two bilinear group of order **p** (p - prime),

And **g** is generator group $\mathbf{G_1}$:

Now we assume a mapping equation e: G1xG2→$\mathbf{G_2}$ is bilinear mapping;

Where d is threshold value.

The general scheme consists of four stages, for each of them has its own algorithm

Generating the public key and master key

Trusted center selects randomly $t_1,\dots,t_n$, y from finite field Z_q and calculates the public key.

$$PK=(T_1=g^{t}{}_{1},\dots,T_n=g^{t}{}_{n},Y=e(g,g)^{y}),$$

Where g is a bilinear group generator

G_1 of order p (p - prime).

Generate private keys

A set of user attributes is supplied to the input of the private key generation algorithm, and the output of the algorithm turns user's private key.

The trusted center generates a private key for each user *U*.

A_U is a set of user attributes. Randomly polynomial *q* of degree *d-1* is selected such that is

$$\boxed{q\ (0) = y.}$$

Private key is $\boxed{D=\{D_i=g^{(q(i))/(t_i)}\}_{\forall i\in AU}.}$

Encryption

The input to the encryption algorithm is fed the message which it is necessary to encrypt, a set of attributes, the owner of which will be able to decrypt the data, and randomly selected number, and the output of the algorithm obtained encrypted data. Owner data encrypt a message $M\in G_2$ using a set of attributes A_{CT} and

A random number $s \in Z_q$:

$$\boxed{CT=(A_{CT}, E=MY^s=e(g,g)^{ys},\{E_i=g^{t_i s}\}_{\forall i\in AU}).}$$

Dencryption

A set of user attributes A_U and the encrypted data are supplied to the input of the decryption algorithm, and the output of the algorithm is obtained decrypted message. If $|A_U\cap A_{CT}|\geq d$, then of $i\in A_U\cap A_{CT}$ selected *d* attributes to compute values

Original message is $\boxed{M=E/Y^s.}$

4. IMPLEMENTATION PHASE

Implementation is the stage where theoretical design is converted into programmatically way. Generally in the implementation stage we will divide the application into number of modules in order to make the application develop very easily. We have implemented the proposed concept on Java Platform in order to show the performance this proposed Achieving Data integrity of Encrypted Cloud Data Using Bloom Filter.The front end of the application takes JSP, HTML and Back-end takes My SQL Server 5.0 along with a Real Cloud Service provider called as DRIVEHQ Cloud Service provider. This cloud service provider will provide a space up to 5 GB for storing the files which is used by the application. The application is divided mainly into following 4 modules. They are as follows:

1. Data Owner Module
2. Authentication Center Module
3. Cloud Server Module
4. Data User

1. DATA OWNER MODULE

In this module, data owner has to register to Authentication Center and Authentication Center checks and authorizes the data owner login . Data owner browse the file , encrypt and upload file with its mac. Once uploaded the file all the authentication center must provide the storage access for the file store on the cloud. Data owner can also delete the file after the uploading of the file to the cloud.

2. AUTHENTICATION CENTER MODULE

In this module Authentication Center checks user & owner login and authorizes the registration. Authentication center list all other sub-authentication centers and provide authorization (Activate OR Deactivate). Authentication center provides the storage access to cloud for every file uploaded by the data owner.

AA 1

In this module the AA1 shows all the private key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

AA 2

In this module the AA2 shows all the public key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

3. CLOUD SERVER MODULE

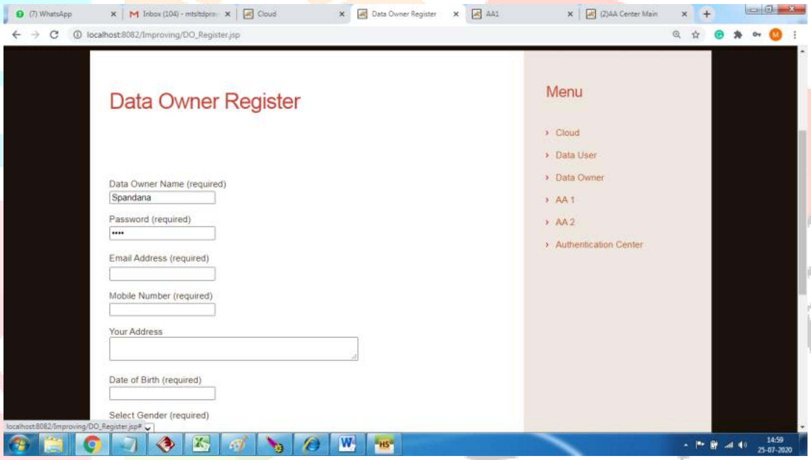
Receive all files from the data owner and store all files, user details. Provide files to end user after verifying Private key and secret key provided by the authentication center. Maintain file transaction details and forward the file download request from the user to the authentication centre.

5. DATA USER MODULE

In this module end user has to register and login, and the user is authorized by the authentication center, user will request private key from the AA1 and the secret key from the AA2 to download the file from cloud server.

5. RESULTS

1) Data Owner Registration



Data Owner Register

Data Owner Name (required)
Spandana

Password (required)
••••

Email Address (required)

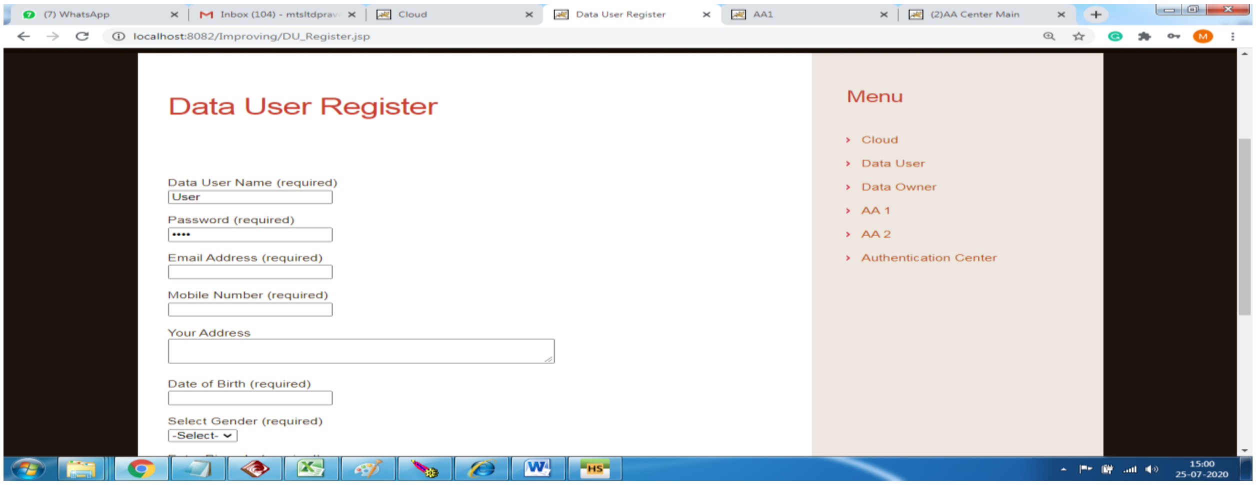
Mobile Number (required)

Your Address

Date of Birth (required)

Select Gender (required)

2) Data User Registration



Data User Register

Data User Name (required)
User

Password (required)
••••

Email Address (required)

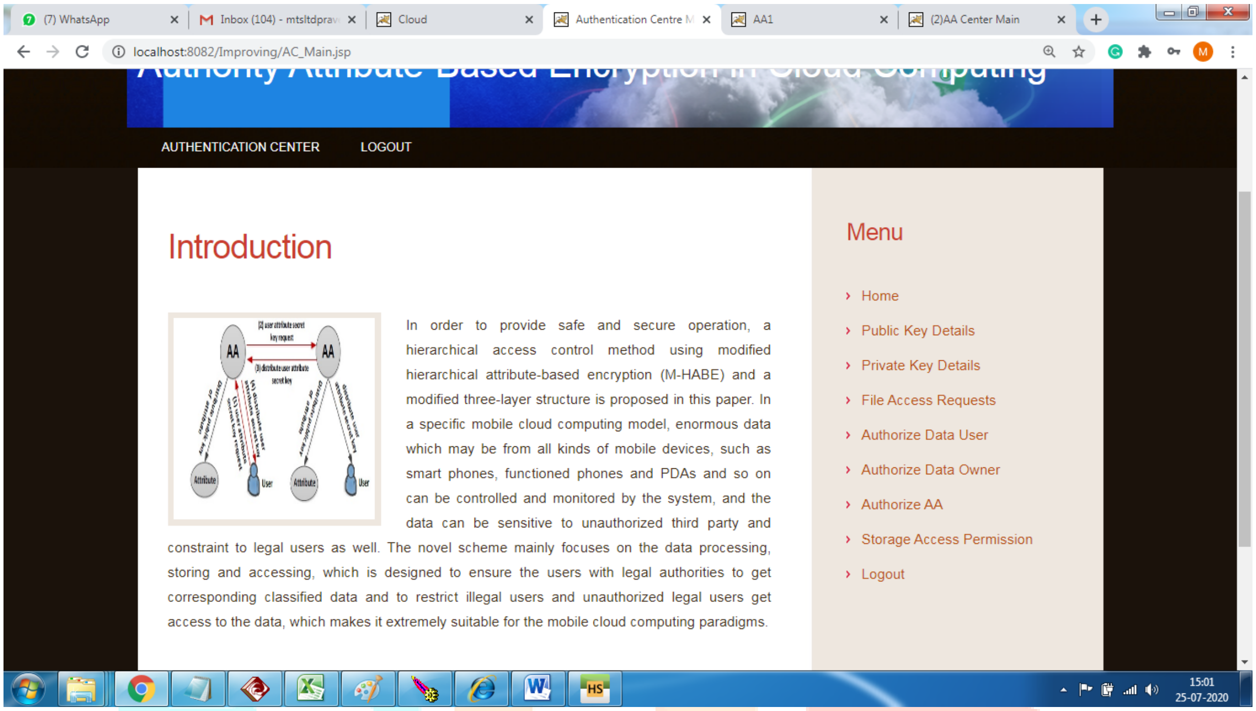
Mobile Number (required)

Your Address

Date of Birth (required)

Select Gender (required)
-Select-

3) Authentication Center Main Page



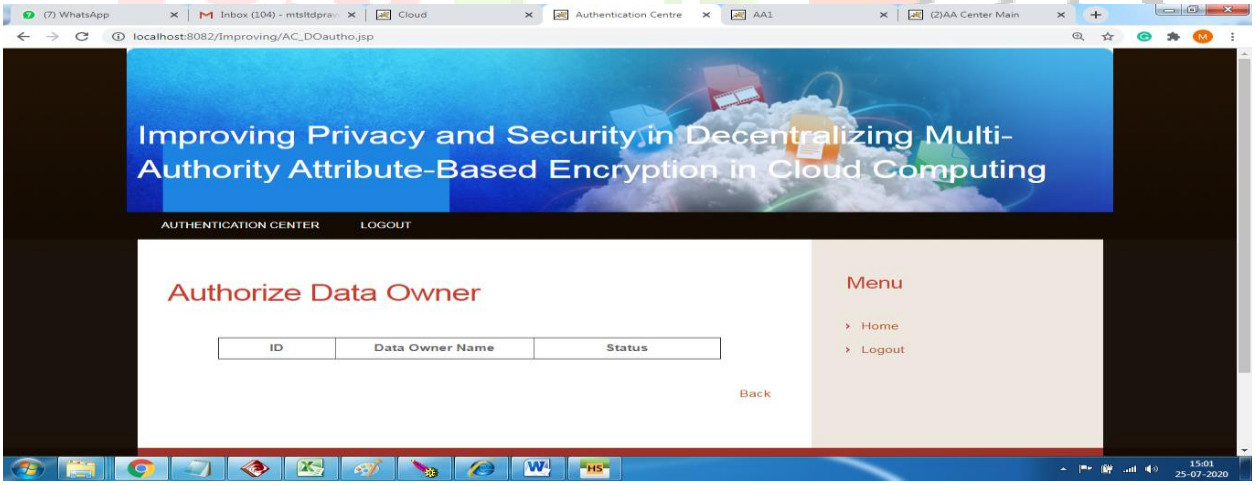
Introduction

In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this paper. In a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms.

Menu

- › Home
- › Public Key Details
- › Private Key Details
- › File Access Requests
- › Authorize Data User
- › Authorize Data Owner
- › Authorize AA
- › Storage Access Permission
- › Logout

4) Authentication Center Authorize Data Owner


(7) WhatsApp
Inbox (104) - mtsltdprav
Cloud
Authentication Centre
AA1
(2)AA Center Main
localhost:8082/Improving/AC_DOautho.jsp
Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing
AUTHENTICATION CENTER
LOGOUT
15:01
25-07-2020

Authorize Data Owner

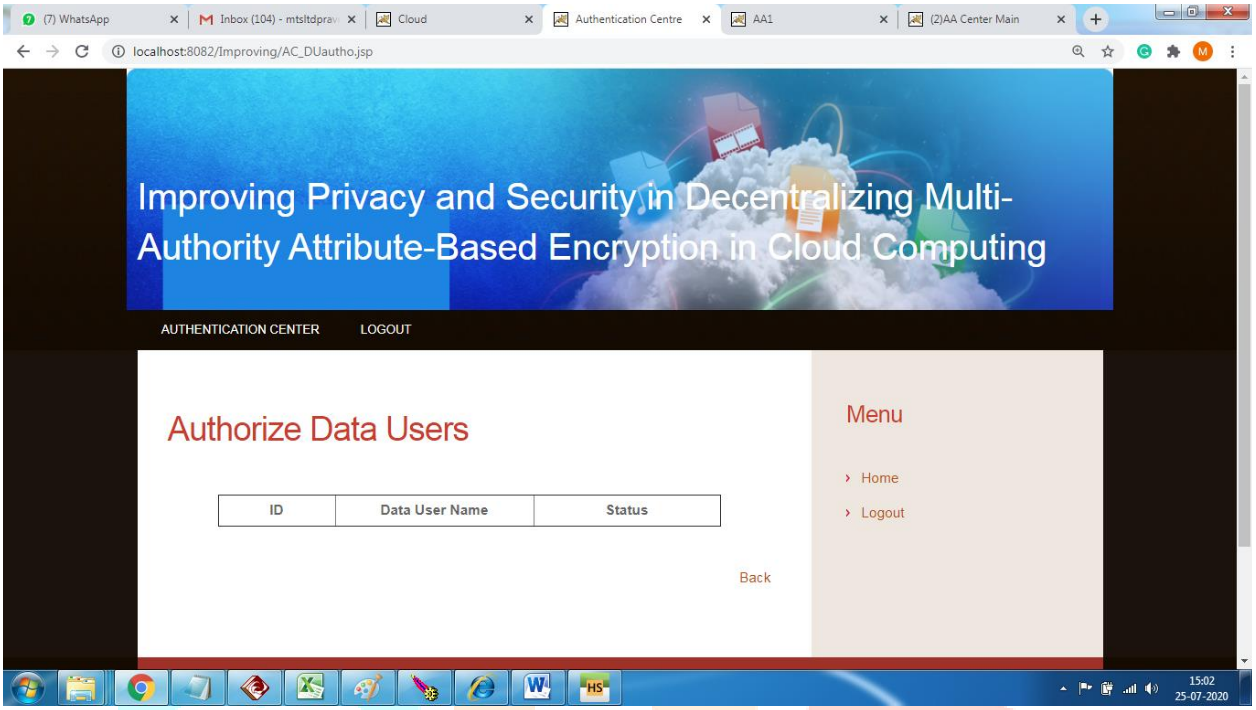
ID	Data Owner Name	Status

Back

Menu

- › Home
- › Logout

5) Authentication Center Authorize Data User



Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing

AUTHENTICATION CENTER LOGOUT

Authorize Data Users

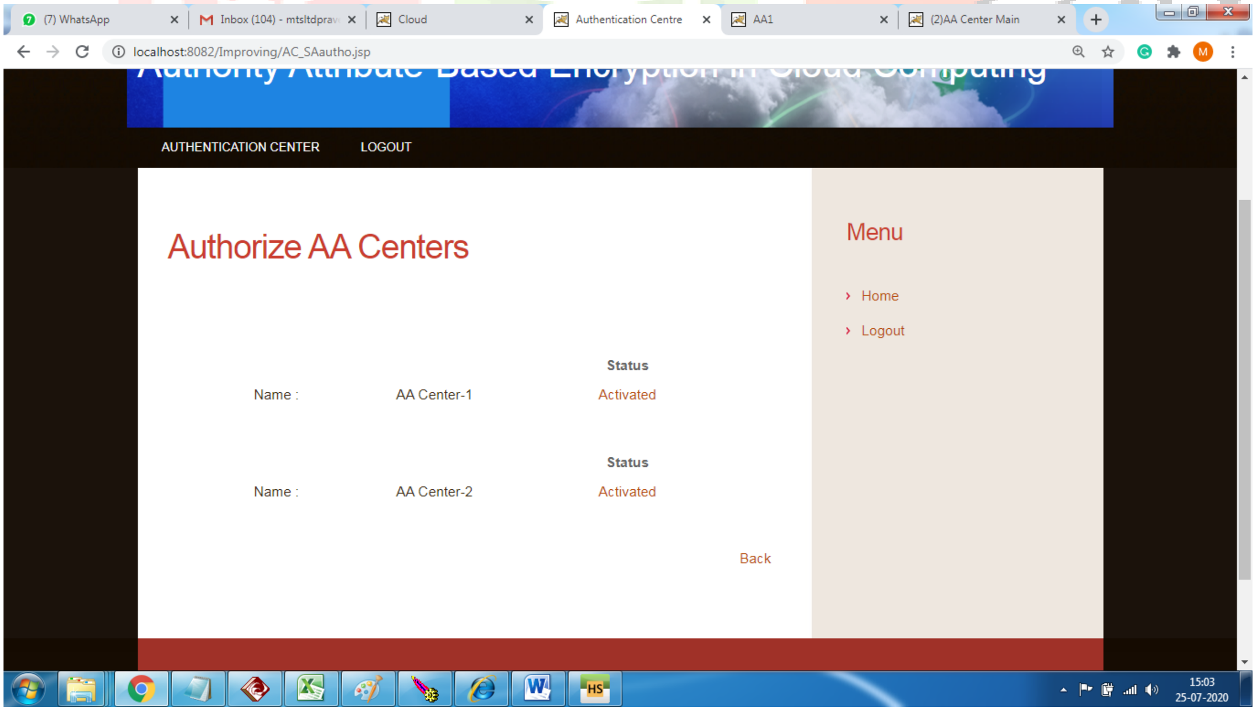
ID	Data User Name	Status

Back

Menu

- Home
- Logout

6) Authentication Sever can See the Activation Status of AA's



Authority Attribute-Based Encryption in Cloud Computing

AUTHENTICATION CENTER LOGOUT

Authorize AA Centers

		Status
Name :	AA Center-1	Activated

		Status
Name :	AA Center-2	Activated

Back

Menu

- Home
- Logout

7. CONCLUSION

In this proposed work we for the primary time designed and implemented a use a third party global identifier in order to verify the key permissions which is granted by the data owner and this will be generating the keys for the data users who try to request the data. In this proposed thesis we try to develop a new scheme by adding a global identifier like Attribute Authority (AA) for providing access keys for the data users who wish to access the sensitive information from the cloud server. In this proposed work we constructed a Composite Order Bilinear Groups scheme for providing access facility for the data users and provide more security for the sensitive data. By conducting various experiments on our proposed model, our simulation results state that proposed system is very efficient to access the data in a de-centralized manner by using a global identifier.

8. REFERENCES

[1] Two Well-known authors J. Horwitz and B. Lynn, has written a paper on "The nist definition of cloud computing," published in http://dx.doi.org/10.602/NIST.SP.800-145.

[2] Two Well-known authors C. Gentry and A. Silverberg, has written a paper on "Hierarchical ID-based cryptography," published in December. 2002.

[3] Two Well-known authors D. Boneh and X. Boyen, has written a paper on "Efficient Selective-ID secure identity based encryption without random oracles," published in Proc.EUROCRYPT, Interlaken, Switzerland, May.2004,pp. 223-238.

[4] Two Well-known authors D. Boneh and E. Goh, has written a paper on "Hierarchical identity based encryption with constant size ciphertext," published in Proc.EUROCRYPT, Aarhus, Denmark, May.2005, pp. 440-456.

[5] Two Well-known authors X. Boyen and B. Waters, has written a paper on "Anonymous hierarchical identity-based encryption(without random oracles)," published in August.2006, pp. 290-307.

[6] Two Well-known authors B. Waters, has written a paper on "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," published in .CRYPTO,Santa Barbara, CA,August. 2009, pp.619-636.

[7] Two Well-known authors A. Lewko, B. Waters, has written a paper on "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," published inProc.TCC,Zurich, Switzerland, February.2010, pp. 455-579.

[8] Two Well-known authors G. Wang and J. Wu, has written a paper on “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” published in.CCS, Chicago,Illinois, USA, October.2010, pp. 735-737.

[9] Two Well-known authors G. Wang,and M. Guo, has written a paper on “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,” published in Computers & security, 30 (5), pp. 320-331, July.2011.

[10] Two Well-known authors Zhiguo Wan, and Robert H. Deng, has written a paper on “HASBE: A Hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” published in IEEE Transactions on Information Forensics and Security, 7(2),pp. 743-753, April.2012.

[11] Two Well-known authors Q. Huang, and Y.Yang, has written a paper on “DECENT: Secure and fine-grained data access controlwith policy updating for constrained IoT devices,” published in World Wide Web, 2017 (11), pp. 1-17, 2017.

[12] A Well-known author A. Beimel, has written a paper on “Secure Schemes for secret sharing and key distribution “published in : Israel Institute of Technology, 1996.