Volume: 5 Issue: XI Month of publication: November 2017

DOI:

Enhanced Novel Multilevel Secure User Authentication Scheme in Cloud.

A.Lakshmi Pavani[1], K.Devi Priya[2]

[1]M. Tech Student, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Peddapuram, East Godavari District, Andhra Pradesh, India.

[2]Sr. Assistant Professor, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Peddapuram, East Godavari District, Andhra Pradesh, India.

Abstract: ***Now a day, cloud computing is becoming more popular and the major problem in cloud computing is security. Many companies such as Amazon, Microsoft are developing cloud computing systems and provide services to large number of users on demand. When we store data in the cloud server some security and privacy issues may take place because many users may use the same server. Some unauthorized users may access the data while storing in the cloud. Unauthorized users may gain the passwords easily because users may not use complicated passwords or may not change the passwords to get multiple services. Hence security enhancement is required such as authentication is provided in this paper. Authentication is the process of checking the identity of the user who is logging on the network. The credentials of the user are compared with the details of authorized users stored in the database; if the user is authorized then he gets the permissions to access the data. Authentication allows the system to identify the user through user id and verify with password. In this paper to provide authentication different levels of authentication centers are available which generates keys to provide security. Encryption algorithm such as AES 256 is used to encrypt the file and store in cloud which provides high security. The evaluated results are implemented using Drive HQ cloud***

Keywords-Cloud computing, Authentication, Security, Authentication center,Sub Authentication centers,AES.

I. INTRODUCTION

Cloud computing refers to sharing and storing information in the cloud. Sharing resources, software and information over the internet. The data which is stored in the cloud server is maintained by cloud service provider. User can use the information stored in the cloud. There is no need to store the information on our own device. One can access files from any location. Users can download the files from the cloud server to any devices such as laptop, tablet or smart phone etc. The price will change depending upon the service used by the user. For example initial amount of 5Gb is free with icloud for storage of data. For additional storage need to pay fee. Cloud computing simply states delivery of computing resources such as servers, storage, databases, networking, software via internet as pay per use [1]. Advantages of cloud computing are world wide access, more storage, easy set up, automatic updates and reduced cost. Companies which provide the services required for the end users are called cloud service providers. Amazon Web Services, Microsoft Azure, Google Cloud Platform, Adobe, VMware, IBM Cloud, Sales force, Oracle Cloud, Verizon Cloud, Drop box are some of examples of cloud service providers. Microsoft Azure is an operating system of cloud and a platform to develop applications in cloud which is used to provide runtime environment for web applications and distributed applications. Google app engine is a scalable runtime environment used for executing web applications. Three delivery models of cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service which are offered based on different services.

A. Services of Cloud

1) *Infrastructure as a Service (IaaS):* This service provides the infrastructure in a virtual environment so that many users can access this service. Resources like Servers, Operating Systems, Virtual Machines, Networks, and Storage etc are provided (e.g. Amazon Web Service, Microsoft Azure).
2) *Platform as a Service (PaaS):* This service provides the environment in which users can compile and run the programs. This service is mainly used by developers.
3) *Software as a Service (SaaS):* It provides application software as pay per use to the end users. It is platform independent and not needed to install software on our own device. This service is available to many end users which makes cloud computing cheap (e.g. Google Applications, Sales force [2]).

B. Characteristics of cloud computing

1) On demand self service means services such as email, applications, server service or network are provided by cloud service providers like Amazon web services, Microsoft, Google etc.
2) Resource polling where polling is grouping of resources. Resource pooling means resources are pooled to serve many end users. Some of the resources are storage, processing and memory etc. Resource pooling leads to high resource utilization rates and economies of scale.
3) Rapid Elasticity in cloud computing is used to provide scalable services. The purpose of elasticity is to avoid over or under-provision. Over provision means assigning large amount of resources than required. Under provision means assigning less resource than required.
4) Measured service means resource usage of Cloud computing can be measured, controlled, and reported. Cloud computing services enable to control and optimise resource usage means pay per use .If one uses more resources need to pay more [3].

The following diagram shows System architecture of cloud computing:

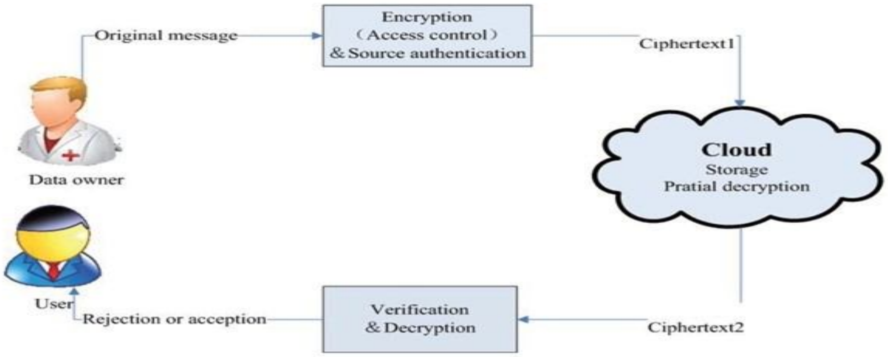


Fig.1 Cloud model to store data in the cloud server.

C. Assume that, in our application the following users are considered

1) *Data owner*- Stores the file in the cloud server in the encrypted form.
2) *Cloud service provider*-Provides the storage infrastructure for data owner on payment basis. Cloud service provider coordinates authentication center to verify the authorized users for accessing data from the cloud.
3) *Data users*- Access data from the cloud server.
4) *Authentication Center* –AuC is trusted by all data owner, data user and cloud service provider which is used to verify whether the requested user is authorized or not.
5) *Sub-Authentication Centers*- Sub-AuC's are used to generate keys in hierarchical level to provide more security.

The remaining sections are organized as follows. Section 2 describes related work. Section 3 provides proposed work. Section 4 shows experimental results. Section 5 contains conclusion.

II. RELATED WORK

Shamir [4] proposed the concept of Identity Based Encryption which is the public key encryption in which the public keys are attributes of user's identity(email address, phone number or biometric data).Sender need to know the receiver's identity which is the public key in order to send an encrypted message. Private Key Generator generates the private keys. Receiver authenticates to an authority and obtains private key corresponding to this id. Receiver decrypts the message using private key over secure channel in order to get plain text. The problem with IBE is PKG generates private keys for users so that any message can be decrypted without authorization.PKG becomes too slow process and expensive computationally and must establish secure channel to transfer private keys. Hierarchical identity based encryption was proposed by Horwitz [5][6] which consists of root PKG. Root PKG generates private keys to domain level PKG's who in turn generates private keys to the users in their domains in the next level.

Pandey [7] proposed the Attribute Based Encryption. The aim of attribute based encryption is to provide security and access control. Based on attributes the encryption and decryption is performed. It is a public key encryption. The secret key of user and cipher text are dependent on attributes. Cipher text decryption is done if the user key attributes are equal with the cipher text attributes [8]. The problem with ABE is data owner needs to use authorized users public key to encrypt the data. There are two types of ABE 1.Key policy ABE and 2.Cipher text policy ABE. CP-ABE encrypts data based on access control policy over attributes, so that only the users who satisfy this policy can decrypt the data. Hierarchical attribute based encryption[9] is a combination of Hierarchical identity based encryption and cipher text policy attribute based encryption which is used to provide fine grained access control and high performance. HABE combines hierarchical generation of keys from HIBE system and access control property from CP-ABE.

The concept of Password Authentication mechanism [10] was proposed by Nancy Victor. This paper explains about how to provide more security using graphical password schemes. Setting a password using images can be performed. If choosing images while setting the password is same as logging into the network then the user is considered as valid and can access the application. The steps performed are entering a number from rolling numbers, entering alphanumeric and finally entering CAPTCHA for providing security.

III. PROPOSED WORK

In this paper, proposed the authentication, authorization protocol and file encryption scheme to store file in the cloud server and to download the file from the cloud server in the secure way. The proposed scheme describes how to secure the data which is stored at the cloud server by using hierarchical structure.

Our Contribution to the proposed work defined as three protocols.

A. Authentication protocol

B. Authorization protocol.

C. File Encryption.

Authentication is the process of verifying the identity of the user to check whether user is valid or not. Authorization Protocol is a cryptographic protocol which is used to perform that specifies what type of resources are accessed by the users. As many unauthorized users may steal the identity of someone hence special verification methods are used to find whether the person is genuine or not. There are many types of authentication protocols some of them are password authentication protocol, challenge handshake authentication protocol, extensible authentication protocol. Encryption is the process of converting plain text into cipher text which is difficult to recognize the data when it is encrypted. It is commonly used to protect sensitive data so that only the authorized users can see it.

Whenever the data owner wants to upload their file in the cloud server in the encrypted format for the security purpose, prove himself as a authenticated user to the cloud server. Then the cloud server allows the data owner to upload the file. The registration phase is required before login in to the cloud. Only the registered users are able to connect with the cloud. In registration, data owner submits the following parameters like name, password, email id, mobile no, address, date of birth, gender, pin code, location, profile picture.

By submitting all the fields data owner will be registered successfully and the acceptance is performed by AuC. Now the data owner is able to upload the file in the cloud server. First selects file which he wants to upload and enters file name then encrypt the file. While encrypting it generates a trapdoor and uploads the file in the cloud server. File will be successfully uploaded in the cloud. Trapdoor is used to encrypt the data with various random possibilities for providing more security for data and same procedure is used to decrypt the data. The login of user and uploading file in cloud steps as follows.

D. Login

1) User Ensures

a) UserName

b) Password

2) UserAction: Send (UserName, Password) to AUC

3) AUC Action:

a) Authentication center Verifies (Username, password)

b) If valid permission granted for uploading the file.

E. Uploading the file in cloud

The following steps are performed during file uploading

1) Select file<-choose file

2) Filename<-Enter file name

3) Key<-Random trapdoor key

4) Cloud<-Send (Encrypt (file, key))

5) Cloud<-Store (file).

F. Key Generation for downloading file

Whenever the data user wants to download the file proves him as an authenticated user, after successful authentication sends request to the AuC. Authentication center is mainly used to provide security. It generates keys so that only the authorized users are able to download the file. The AUC maintains hierarchy of Sub-AuC (Low level Authentication centers) for granting permissions to the users for downloading files. The hierarchy of Sub-AuC is maintained for providing strong security to the data and authenticating users.

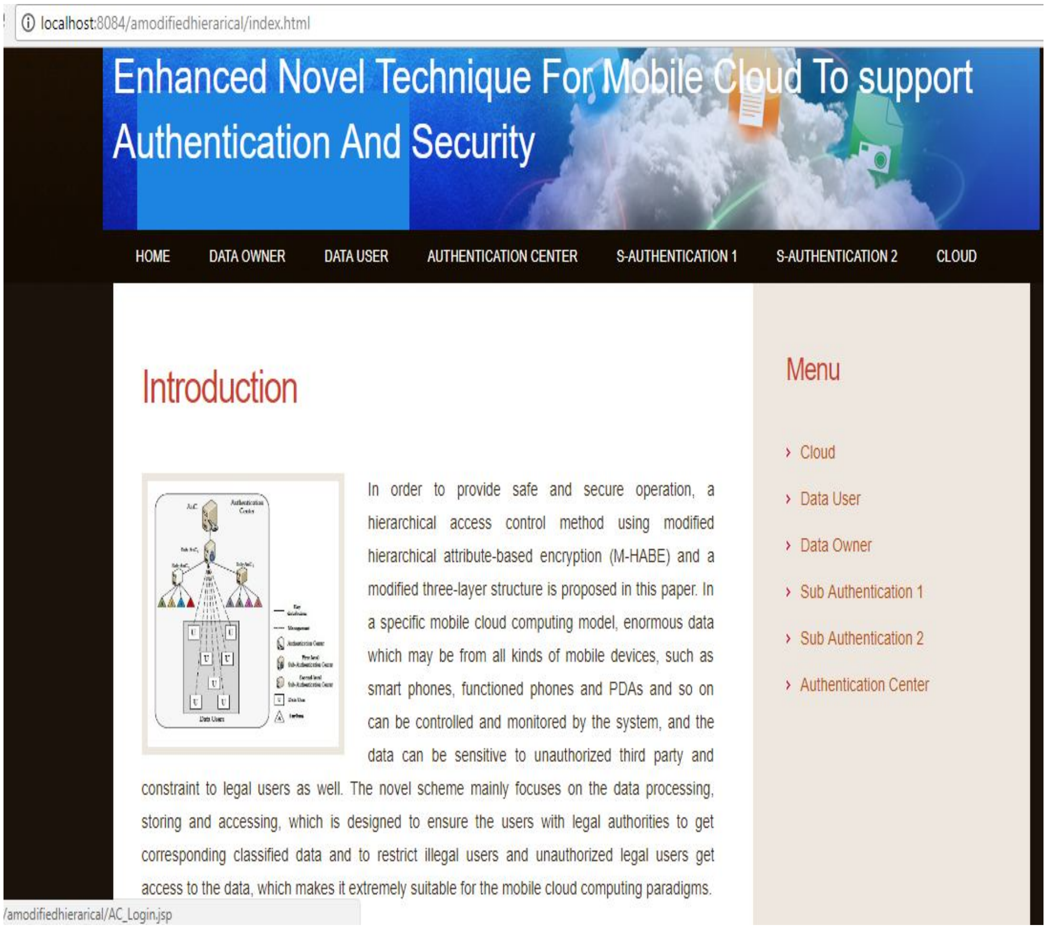
If permissions are provided by authentication center to the user then data user can request the keys. If data user request the key_1 that request will be sent to sub-authentication center2.If user request key_2 that request will be sent to sub-authentication center1.Sub-authentication center1 and sub-authentication center2 will generate the keys key_2 and key_1. Data user can download the file by entering the file name, trapdoor, key_1 and key_2.Hence the file is downloaded from the cloud server.

IV. EXPERIMENTAL RESULTS

The proposed work is implemented by java with Drive HQ cloud. The user interface is created with JSP framework and the files which are uploaded by the data owner stored in Drive HQ cloud with an encrypted format. The standard encryption algorithm AES is used to encrypt the file.

Drive HQ: Free cloud server Drive HQ is used in this project. The storage space provided by Drive HQ is 1gb.Users can easily upload or download files on Drive HQ cloud storage system using Drive HQ file manager, web browser, ftp service or Drive HQ web dav cloud drive. Users can access files from anywhere at any time. Drive HQ requires signup which consists of username, email address and password. If the details are correct one can login and can use the service.

A. Home Page



localhost:8084/amodifiedhierarical/index.html

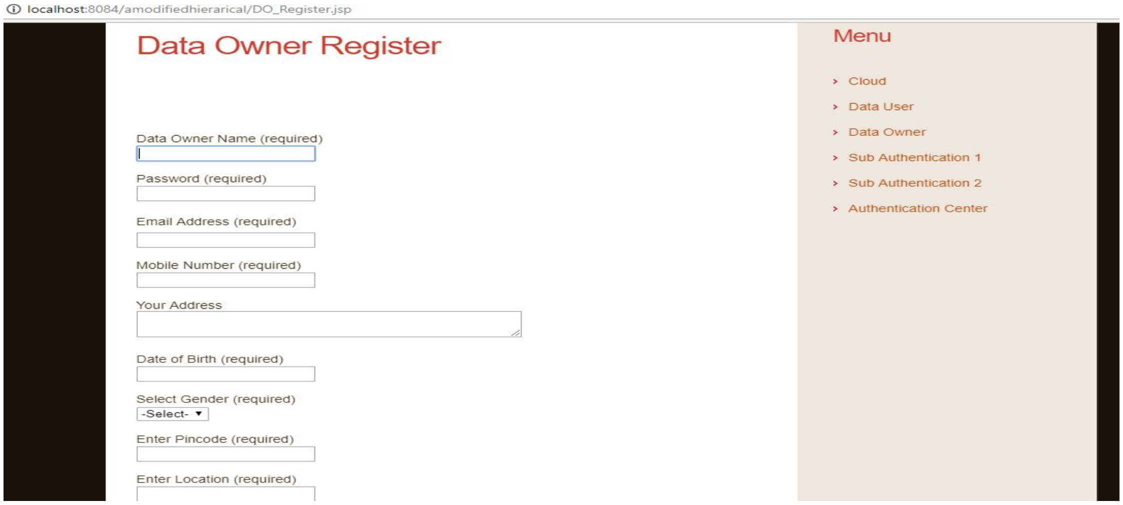
Enhanced Novel Technique For Mobile Cloud To support Authentication And Security

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.

/amodifiedhierarical/AC_Login.jsp

B. Data Owner Register Form



Data Owner Register

Data Owner Name (required)

Password (required)

Email Address (required)

Mobile Number (required)

Your Address

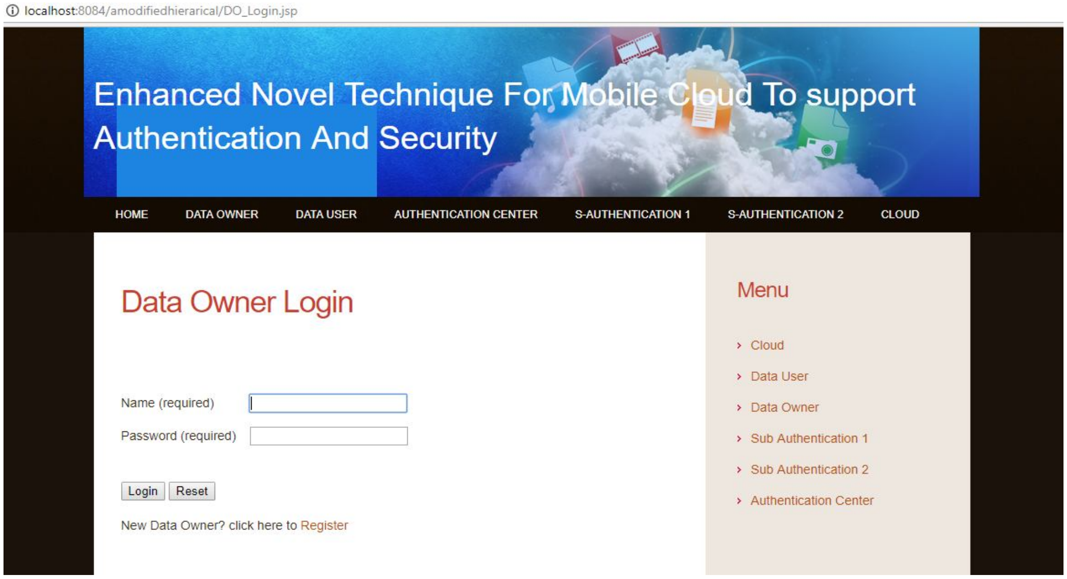
Date of Birth (required)

Select Gender (required)

Enter Pincode (required)

Enter Location (required)

C. Data Owner Login



Enhanced Novel Technique For Mobile Cloud To support Authentication And Security

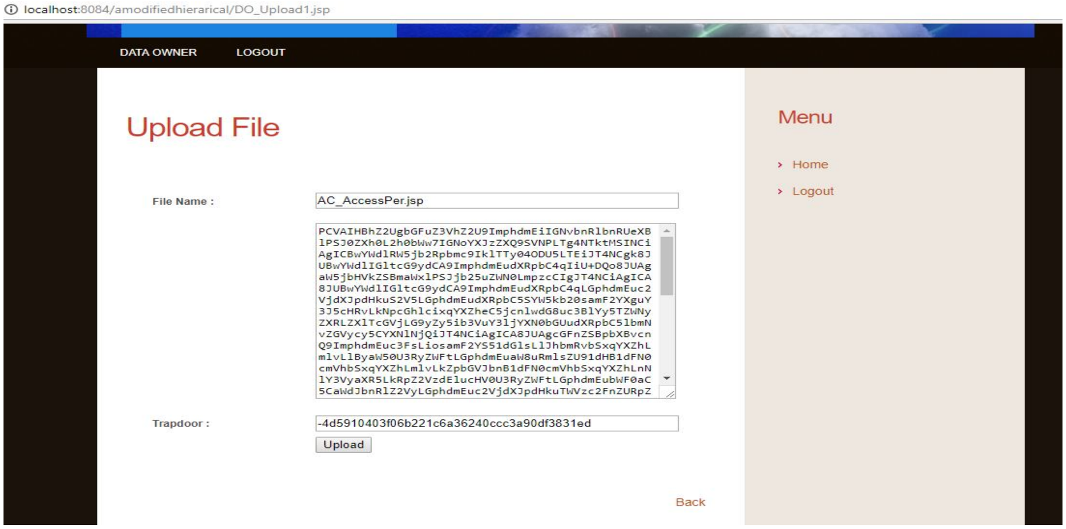
Data Owner Login

Name (required)

Password (required)

New Data Owner? click here to Register

D. Upload File



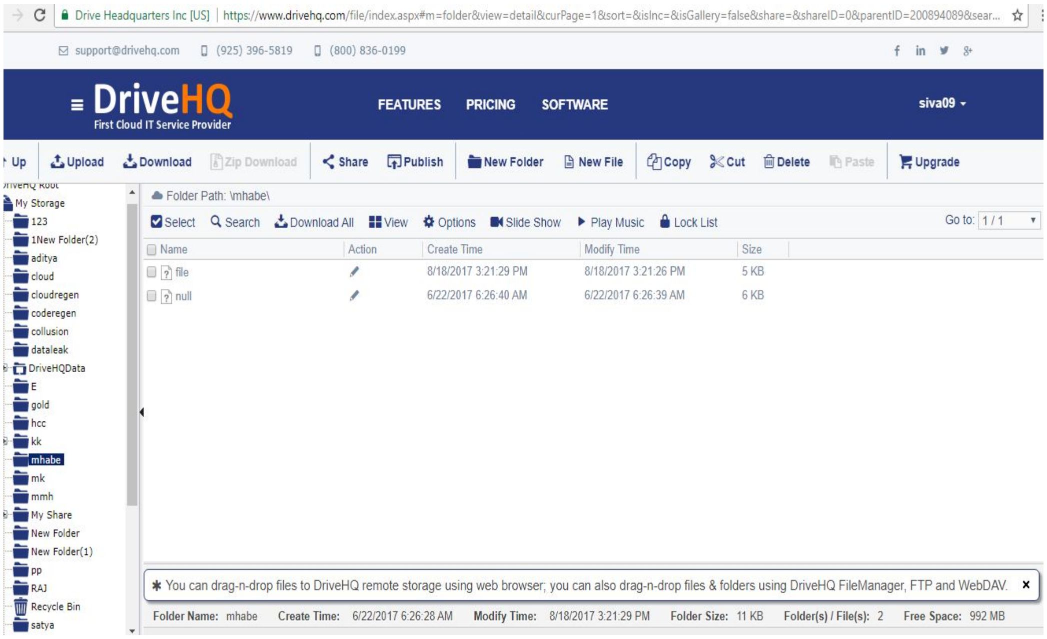
Upload File

File Name : AC_AccessPer.jsp

```
PCVAIHBhZ2UgbGFuZ3VhZ2U9ImphdmEiIGNvbnRlbnRUeXB
lPSJ0ZXh0L2h0bWw7IGNoYXJzZXQ9SVNPLTg4NTktMSINCi
AgICBwYWdlRW5jb2Rpbmc9IklTTy04ODU5LTEiJT4NCgk8J
UBwYWdlIGltcG9ydCA9ImphdmEudXRpbC4qIiU+DQo8JUAg
aW5jbHVkZSBmaWxlPSJjb25uZWN0LmpzcCIgJT4NCiAgICA
8JUBwYWdlIGltcG9ydCA9ImphdmEudXRpbC4qLGphdmEuc2
VjdXJpdHkuS2V5LGphdmEudXRpbC5SYW5kb20samF2YXguY
3J5cHRvLkNpcGhlcixqYXZheC5jcnlwdG8uc3BlYy5TZWNy
ZXRLZXlTcGVjLG9yZy5ib3VuY3ljYXN0bGUudXRpbC5lbmN
vZGVycy5CYXNlNjQiJT4NCiAgICA8JUAgcGFnZSBpbXBvcn
Q9ImphdmEuc3FsLiosamF2YS51dGlsLlJhbmRvbSxqYXZhL
mlvLlByaW50U3RyZWFtLGphdmEuaW8uRmlsZU91dHB1dFN0
cmVhbSxqYXZhLmlvLkZpbGVJbnB1dFN0cmVhbSxqYXZhLnN
lY3VyaXR5LkRpZ2VzdElucHV0U3RyZWFtLGphdmEubWF0aC
5CaWdJbnRlZ2VyLGphdmEuc2VjdXJpdHkuTWVzc2FnZURpZ
```

Trapdoor : -4d5910403f06b221c6a36240ccc3a90df3831ed

E. Store File in drive hq Cloud



Folder Path: \mhabe\

□ Name	Action	Create Time	Modify Time	Size
□ file		8/18/2017 3:21:29 PM	8/18/2017 3:21:26 PM	5 KB
□ null		6/22/2017 6:26:40 AM	6/22/2017 6:26:39 AM	6 KB

✱ You can drag-n-drop files to DriveHQ remote storage using web browser; you can also drag-n-drop files & folders using DriveHQ FileManager, FTP and WebDAV. ×

Folder Name: mhabe Create Time: 6/22/2017 6:26:28 AM Modify Time: 8/18/2017 3:21:29 PM Folder Size: 11 KB Folder(s) / File(s): 2 Free Space: 992 MB

V. CONCLUSION

As Cloud computing becoming fastest growing technology, security plays a major role in cloud. Protection of information from theft as well as data leakage and deletion of information from cloud can be avoided by proving security [11]. Some unauthorized users may gain the information from the cloud hence in this paper, proposed user authentication which provides strong security due to verification done by authentication centres. To provide security data should be encrypted first and need to store in the cloud. AES algorithm is used to encrypt file. Whenever data user wants to download the file authentication centres should generate keys in a hierarchical level which provides strong security. The evaluated results are implemented with JSP framework and Drive HQ cloud.

VI. ACKNOWLEDGMENT

I would like to express my gratitude to my Guide Mrs. K. Devi Priya, M. Tech, Sr. Assistant Professor, without her guidance, this paper is not possible. Her understanding encouragement and personal guidance have provided the basis for this paper.

REFERENCES

[1] J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser, "Cloud Computing Basics," International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 5, ISSN : 2278 – 1021 ,July 2012.

[2] Rahul Bhoyar, Prof.Nitin Chopde,"Cloud Computing:Service models,Types,Database and ssues," Volume 3, Issue 3, ijarcsse, ISSN: 2277 128X ,March 2013 .

[3] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong," The Characteristics of Cloud Computing," 2010 39th International Conference on Parallel Processing Workshops.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[5] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in Advances in cryptologyASIACRYPT 2002. Springer, 2002, pp. 548–566.

[6] J.Horwitz and B.Lynn,"Toward hierarchical identity-based encryption," in Advances in CryptologyEUROCRYPT 2002. Springer,2002, pp.466– 481.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.

[8] I. Stojmenovic, "Access control in distributed systems: Merging theory with practice," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE, 2011, pp. 1–2.

[9] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 735–737.

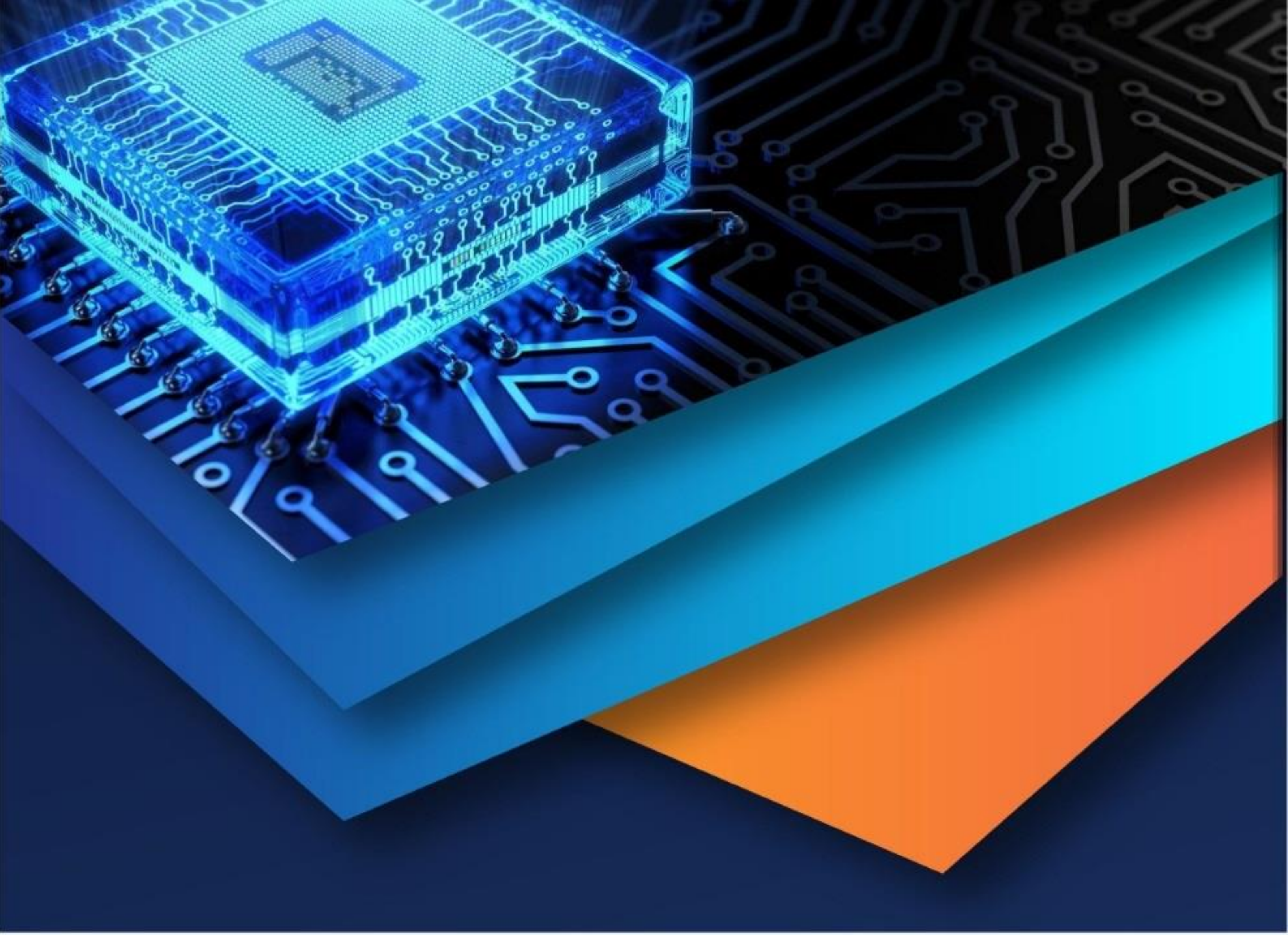
[10] Nancy Victor," A Novel Graphical Password Authentication Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 9, September 2014, ISSN: 2277 128X.

[11] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010, pp. 105–112.

AUTHORS PROFILE

A.Lakshmi Pavani received the B. Tech. Degree in Electronics and communication Engineering from Sri Prakash College of Technology,permanently affiliated to J.N.T.U. Kakinada, Andhra Pradesh, India. Presently working for M. Tech. Degree in Computer Science and Engineering at Aditya Engineering College, affiliated to J.N.T.U. Kakinada, Andhra Pradesh, India.

Mrs.K.Devi Priya obtained her M.Tech Degree in Computer Science from Jawaharlal Nehru Technological University,Kakinada.And pursuing Ph.D from JNTUK.She had teaching experience of 10 years. She is currently working as Sr.Assistant Professor in CSE at Aditya Engineering College,Surampalem,Andhra Pradesh,India.She taught subjects like Information Security,Database Management,Big data,Hadoop,Web Technologies and Operating systems. Her research interests include Cloud Computing,Network Security,Big Data.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY