International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Common Cloud Interface

Author 1: Mr. A.Venu Gopal Rao, M.Tech, (P.h.D)
(Associate Professor, Department of Computer Science and Engineering, Sphoorthy Engineering College, Hyderabad.
Email: venugopal299@gmail.com
Author 2: Karanam Srivardhan, B.Tech
(Student, Department of Computer Science and Engineering, Sphoorthy Engineering College, Hyderabad.
Email: vardhankaranam25@gmail.com
Author 3: Pothula Sree Uday, B.Tech
(Student, Department of Computer Science and Engineering, Sphoorthy Engineering College, Hyderabad.
Email: sreeuday789@gmail.com
Author 4: Rakonda Akshaya, B.Tech
(Student, Department of Computer Science and Engineering, Sphoorthy Engineering College, Hyderabad.
Email: akshaya1122reddy@gmail.com

I. ABSTRACT:

Cloud these days is everywhere. Users are increasing day by day which reduces the privacy that the cloud has. In view of that, an interface that has access to all cloud vendors is designed such that it promotes privacy by segregating users of any cloud into data owners and data users where the data owners are the ones who have created/uploaded any file and data users are the other cloud users that are in the cloud space alongside.For the privacy of the data owner, the access to his files is to be limited but in the current situation, the file can be accessed by all his co-cloud users. By using this web interface to upload the file into any cloud service the file will be encrypted first by the interface and then will be stored in the intended cloud storage this makes all the co-cloud users unable to access it. When requirements come such that any other user should access the file then this interface provides an option for them to request the access to this file and the owner has the decision to make based upon which the access is controlled. Privacy is enabled for the owner of the file.Other features include user-friendliness where everything is done by the interface the process of encryption, decryption will be handled by the interface with no input needed from the owner or user making the interface highly friendly to any sector of people.

Keywords: Cloud, Encryption, Decryption, Interface, Privacy, User-Friendly

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

II. INTRODUCTION:

Protective pieces of the action are a great start for protecting Files in the cloud, but providing a mechanism when a gainful offense hits are also equally significant. The major aim of this web interface is to provide a solution to the attacks of other users on the files. It provides security for various users of the files. It protects your file from being harmed by the other people. Today Encryption techniques are used by various businessmen and also cloud users to hide data from various evil users. Usually, this technique could be a burden to the user if he forgot his generated private key. The prime advantage of this Interface is that everything will be done on its own no Instruction or private key, is needed from the user this makes This interface user-friendly, and the content inside your cloud is also safe.

Encryption of files helps the one last saving grace, the data may be present in your cloud but it will not allow the other one also to use it. Encryption gives an extra added layer of security to make you feel secure even if your cloud is shared. Information hiding is the mechanism for protecting the given content of data from modification. It reduces software development risk by depending on the key generation technique. File Encryption is the better easy and more efficient style for accomplishing data security. To glance at an encrypted file, you must approach the user of the file to decrypt it.

It is the process of hiding the text file details. The hiding of these details results in abstraction, enables privacy in the cloud and it helps to lower the external complexity and make the function easy for us.

III. LITERATURE SURVEY

The aim of the web application mainly focuses on the concern about solutions to privacy that include policy and legislation as well as end-user choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. Identity Management Issues can also provide practical solutions to privacy concerns in cloud computing. These systems distinguish between authorized and unauthorized users and determine the amount of data that is accessible to each entity. The systems work by creating and describing identities, recording activities, and getting rid of unused identities. The prime advantage of file encryption is that even if you are about to lose your computer or laptop or get attacked by noxious malware or if your laptop is hacked, the content inside your laptop is still safe. It reduces software development risk by depending on the key generation technique. File Encryption is the better easy and more efficient style for accomplishing data security. To glance at an encrypted file, you must approach the secret key to decrypt it. It is the process of hiding the text file details. The hiding of these details results in abstraction, it helps to lower the external complexity and make the function easy for us.

IV. IMPLEMENTATION:

The core of this project is about working with different cloud providers and executing the same for every cloud.Here is a sample code of using Amazon Web Services SDK to upload any file into S3 bucket using the interface.

```
import java.io.File;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.services.s3.S3Client;
import
software.amazon.awssdk.services.s3.model.PutObject
Request;
public class Amazon {
public void upload(String f) {
String path = "/Users/vardhankaranam/tomcat/apache-
10.0.27/files/";
S3client cli= S3Client.builder().build();
PutObjectRequest.builder().bucket("bucket1").key(f).buil
d();
 cli.putObject(req, RequestBody.fromFile(new File(path +
f)));
}
}
```

Amazon SDK has to be imported for utilizing their classes for that the import statements of AWS are written at the top followed by the class(Amazon) which uses these classes of AWS the method upload takes the file that has to be uploaded into the bucket this file is already encrypted in the previous

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

step.The bucket name in this instance is “bucket1” which is already created using AWS SDK methods the bucket is accessed from this code and the encrypted file is uploaded.

V. RESULTS:

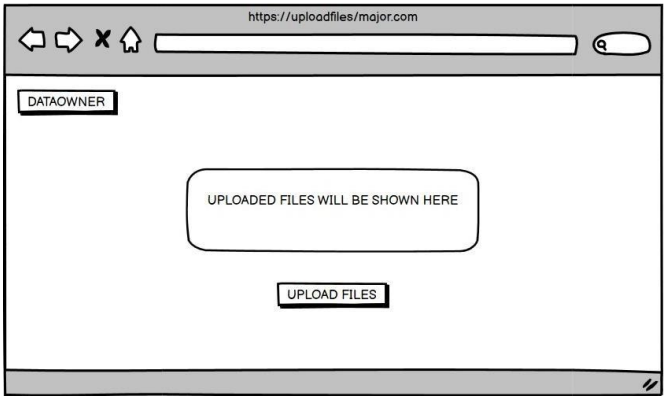

Fig 1: Upload Files

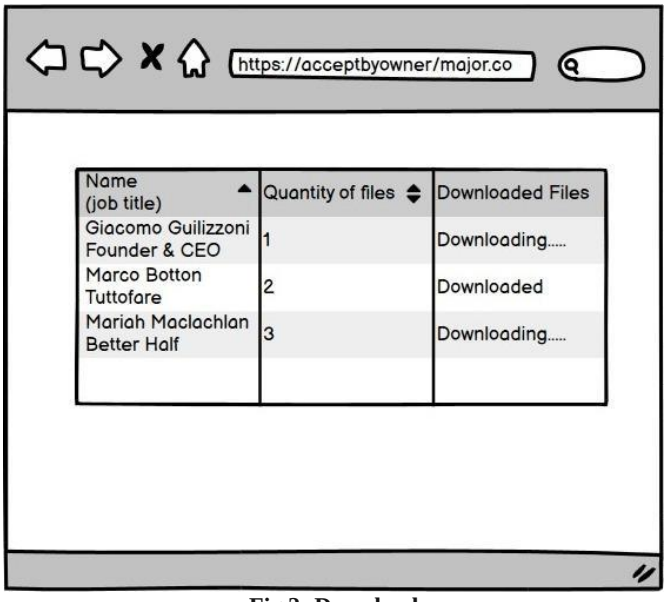

Fig 2: Download

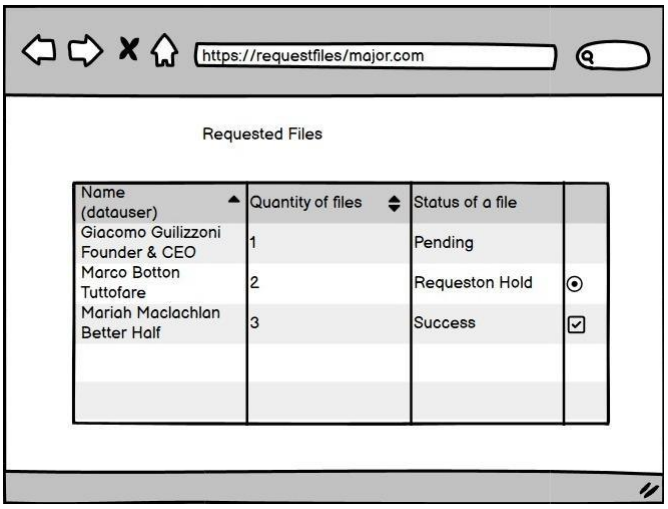

Fig 3: Request

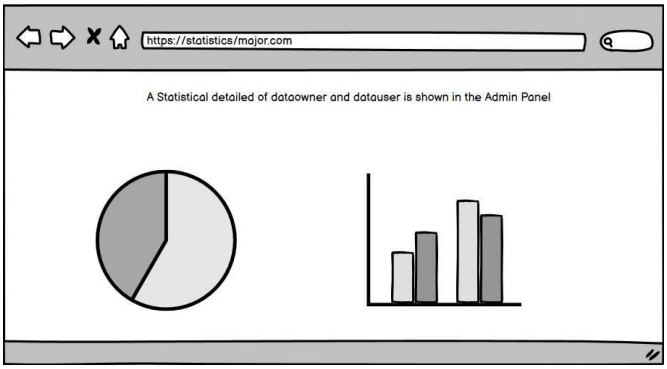

Fig 4: Statistical details of data owner and data user

VI. CONCLUSION:

Common cloud interface deals with the concepts of security of digital data communication across the network. The method proposed has proved successful in hiding various types of text, images and documents by using encryption methods. We concluded that in our method the text files and images are encrypted and the usage of private and public keys are better techniques. Results achieved indicate that our proposed method is encouraging in terms of security and robustness.

VII. ACKNOWLEDGMENT:

This work has been carried out as part of our academic project to be submitted to the university. In this project work, we got the guidance and all inputs from our internal guide Mr.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

VenuGopal and we are thankful to our guide for his constant support and encouragement without which, the paper could not be completed.

VIII. REFERENCE

[1] H.Abdulzahra, R. AHMAD, and N. M. NOOR, "Security enhancement; Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp.978-960,2014.

[2] P. R. Ekatpure and R. N.Benkar, "A comparative study of steganography & cryptography,"2013.

[3] M. H. Rajyaguru, "Cryptography-combination of cryptography and steganography with rapidly changing keys ," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp.2250-2459,2012.

[4] D. Seth. L. Ramanathan, and A. Pandey, "Security enhancement; Combining cryptography and steganography," International Journal of Computer Applications(0975-8887)Volume,2010.

[5] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image steganography," International Journal of Computer Science and Network Security(IJCSNS), vol. 14, no. 6. P. 58. 201.