Efficient Cloud Storage Using Encryption Mechanism

Priyanka G. Rathod,
Computer Science and Engineering,
Jspm's ICOER,
Pune, India

PiyushThada,
Computer science and Engineering,
Jspm's, ICOER
Pune, India

Aishwarya Mule,
Computer science and Engineering,
Jspm's, ICOER,
Pune, India

DikshaWagh,
Computer science and Engineering,
Jspm's, ICOER,
Pune, India

Guide Name: Prof.Krishna Kulkarni
Computer Science and Engineering
Jspm'sICOER,Pune, India

Abstract*— *Cloud computing is something which is executed to remedy the computing problems faced in day to day life. It is nothing but a unreal and a virtual pool of some resources allotted or served to us through the internet when and where required. Cloud Computing has so much to offer as its services. One of such is SAAS which is Storage as a Service. And The Storage Service of a Virtual Cloud has become very much popular these days for both commercial as well as personal use. As it is so much popular, it is very essential to provide some kind of security to it. Hence, in this paper, we are basically encrypting the data which is being stored on the cloud. So instead of storing it directly, we first encrypt it and then store it. We have used TRIPLE DES Algorithm to store the data efficiently and securely at the same time.

INTRODUCTION

Cloud computing is a "new" computer model that allows using remote services through a network using various resources. It is basically meant to give the maximum capacity with the minimum resources. The end user has the minimum hardware requirement, but he uses the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. One of such services is data storage.

Our system provides you a cloud platform wherein you can store your files and simply your data in a secure way. And these files can be of various multiple extensions such as Text Files, Word Documents, PDFs, Images, etc.

So, as discussed above our proposed system s just more than a typical cloud service. It is a much secure and much reliable cloud storage system in today's world. The main reason of such system to come into existence is that the consumers hesitate to store their precious data over the cloud as it is more of an open source platform and its vulnerabilities can be easily exploited if compared to any other typical file storage system. So for the encryption part, we have used TRIPLE DES algorithm with 192-bit (24*8) encryption key structure along with a password phrase to make the system as well as the algorithm more secure. We are using Triple DES algorithm specifically as it is much more secure than single DES. And talking about other algorithms, they are at the most 128-bit encryption specific. But as we now know, this isn't the case with Triple DES as it supports up to 192-bit of encryption.

RELATED WORK

Managing the user data of such sensitive data with various extensions becomes very complex. The major advantage of the proposed system is obviously the security which makes it reliable and secure to operate. The other basic advantage being you can store all our data in one place without a need to maintain different sources for every file type or simply application specific files. So by using this mechanism of the proposed system you can access all your data in one place at your fingertips. Also here we don't just use a homomorphic encryption technique. In fact, we combine it along with a password phrase which makes it comparatively reliable for use.

Here the main concern is security as cloud is more of an open source platform. So we will have to consider all the security aspects and concerns when talking about cloud. We provide a set of steps where we describe the actual working of the proposed system. We will be discussing the same further.

PROPOSED SYSTEM

The proposed system makes use of Triple DES Algorithm to encrypt the data and hence allow the user to download the files in both encrypted and decrypted formats. Herein, the basic algorithmic steps would be as follows. In the very first step, the user will upload his/her data. In the next step, this data will now be encrypted with Triple DES Algorithm with 192-bit encryption. The proposed system architecture is shown in fig 1.

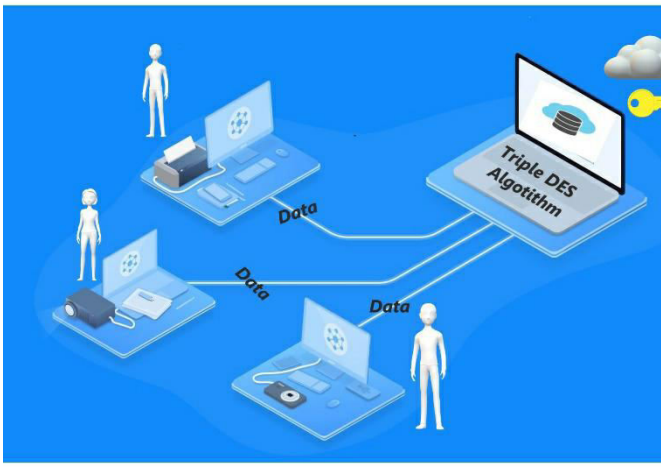


Fig 1. Proposed System Architecture.

The system we are proposing in this system aims to address the issues of cloud security. So along with the 192-bit encryption it also assigns & hence combines a password phrase which would now make the encryption algorithm much more secure now.

Modules and Working of Proposed System:

1. User Registration:

The very first step in the proposed system would be user login. This is the initial stage where the user is redirected to a registration page and user details are taken as input to hence create a user account in our cloud storage eco-system. Once the account is created user can now perform file operations with the same account.

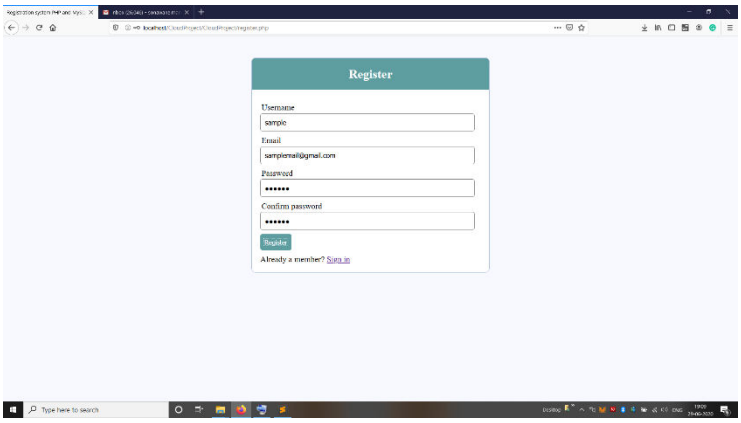


Fig 1. User Registration.

2. User Login:

This is the next step in the proposed system where user logs in to his / her account which was created in the previous step by hence entering valid credentials for the same. Once login successful, the user is redirected to the dashboard page where he / she can perform various file related operations like upload file, download decrypted file, download encrypted file etc. Else in case of invalid credentials, the login fails and user stays on same screen.

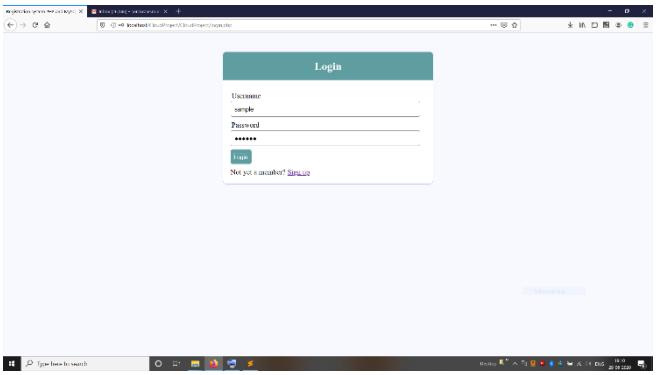


Fig 2. User Login.

3. File Upload:

The system consists of a module wherein it allows the user to upload his / her documents and files. This is the very first step to upload the data to the cloud. And the user can upload multiple types of file extensions here such as .docx, .doc, .txt, .pdf, .jpeg, .jpg, .png, etc.

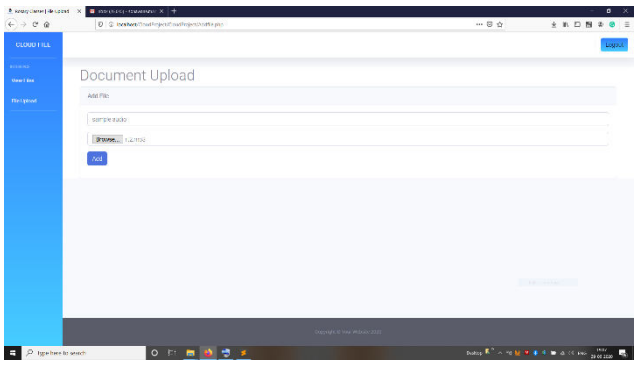


Fig 3. File Upload.

4. Encryption Process:

The system consists of a module wherein it allows the user to upload his / her documents and files. This is the very first step to upload the data to the cloud. And the user can upload multiple types of file extensions here such as .docx, .doc, .txt, .pdf, .jpeg, .jpg, .png, etc.

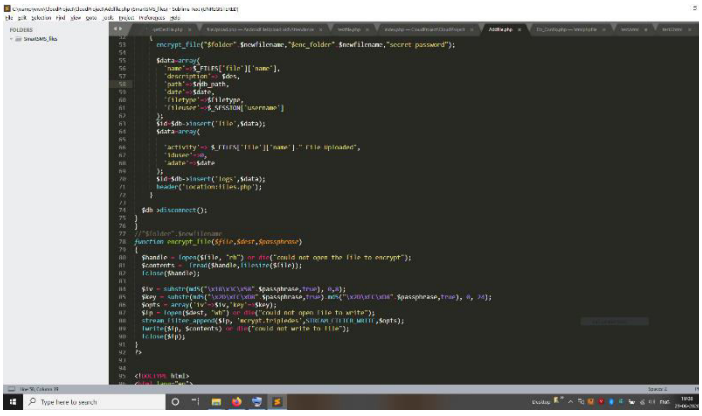


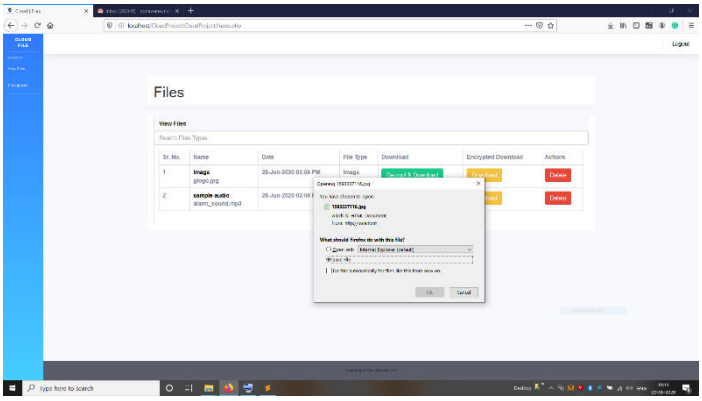
Fig 4. Encryption Process.

5. Encrypted & Decrypted Downloads:

Once the file is encrypted and uploaded the user now has options to:

5.1 Download the Encrypted File:

Here, the file which was encrypted in step 4 can now be downloaded in the same encrypted format and hence the original content cannot be viewed due to encryption procedure.



5.2 Download the Decrypted File:

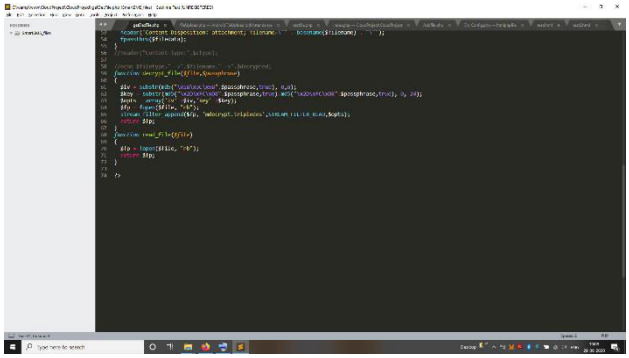


Fig 5.2.a Download Decrypted Process.

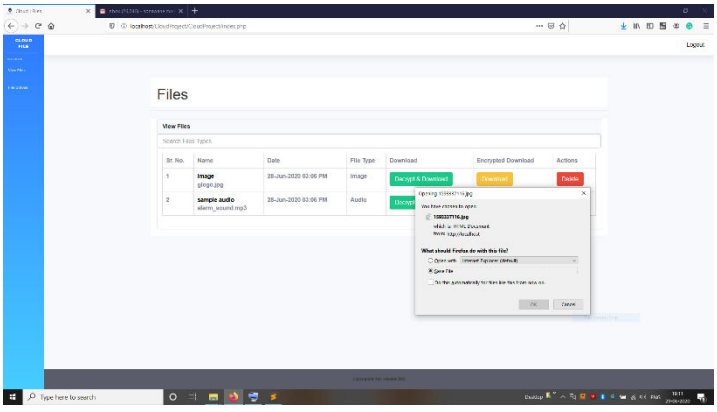


Fig 5.2.b Download Decrypted Process.

Here, Fig 5.1.a shows the process of decryption and exactly how it is done. Which is simply the reversal of encryption process by decrypting and removing password phrase from the encrypted data. And Fig 5.1.b shows the output for the same.

6. View Files:

The system consists of a module wherein it allows the user to view his / her documents and files when and where required as per the requirements. This access would be user specific. Means the user can only delete the files uploaded by that particular user. This improves security & privacy concerns at the same time.

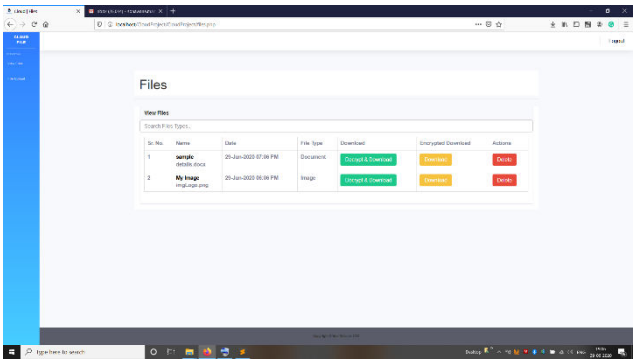


Fig 6. View Files.

MATHEMATICALMODEL

Set theory of the proposed system:
S = {I, P, O}
I= Input to the System.
P= Processing of System.
O= Output of the System.

I = {i1, i2, i3}
i1 = Registration.
i2 = Login.
i3= File Upload as input.

P = {p1, p2, p3}
p1 = Applying Triple DES Algorithm.
p2 = 192-bit encryption.
p3 = adding password phrase.

O= {o1, o2}
o1= Encrypted File Download.
o2= Decrypted File Download.

7. RESULTS OF SYSTEM

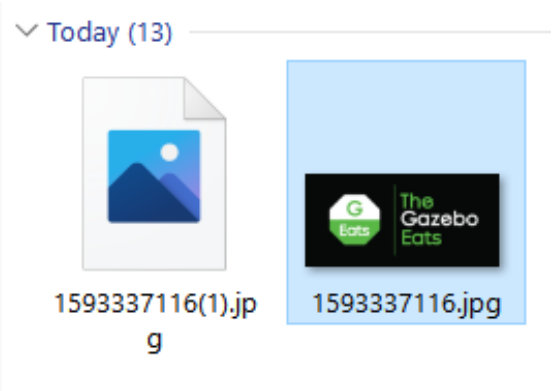


Fig 7. Encrypted & Decrypted Outputs.

APPLICATIONS

1. The proposed system can be used in personal computers to store data more securely.
2. It can be used in Corporate world like in banks, IT firms wherein arrival time plays a vital role.

1. CONCLUSION

Thus, the survey on efficient cloud storage using encryption mechanism depicts the use of encryption techniques using Triple DES Algorithm which securely store data. The use of a secret key i.e. password phrase makes the system much more secure. Many of the existing systems in the literature proposed the system do not really achieve such accurate results for achieving the desired results. So, to overcome, this above framework is the better and reliable solution from every perceptive of security. In this way we have accomplished to add to a reliable and effective data encryption framework to secure the user data in a reliable way.

Thus, there is a need of an efficient system which will not only save the user privacy but will save provide more security as well.

ACKNOWLEDGMENT

The All faith and honor to our HOD for his grace and inspiration. I would like to thank all my Friends and Family members they were always been there to support us. We sincerely thanks to our Department Head, Project coordinator, our project guide and all other staff members to give us the guidelines for this paper.

REFERENCES

[1]. https://en.wikipedia.org/wiki/Apache_Hadoop

[2]. Louis Columbus, “Analytics, Data Storage Will Lead Cloud Adoption In 2017”, Forbes, Nov 20, 2016

[3]. Websource:https://www.forbes.com/sites/louiscolumbus/2016/11/20/analytics-data-storage-will-lead-cloud-adoption-in-2017/#74e63c357e7a

[4]. Robert McMillan, "Capital One Breach Casts Shadow Over Cloud Security", The Wall Street Journal, July 30, 2019

[5]. Web source: https://www.wsj.com/articles/capital-one-breach-casts-shadow-over-cloud-security-11564516541

[6]. Ibrahim AbakerTargioHashem et al, "The Rise of Big Data on Cloud Computing: Review and Open Research Issues", Information Systems,Vol. 47, pp. 98-115, 2015

[7]. " Top Threats to Cloud Computing the Egregious 11", CSA Report, 2019

[8]. Govind Rao Mettu1 and Dr. AnithaPatil, "Data Breaches as Top Security Concern in Cloud Computing", International Journal of Pure and Applied Mathematics, Vol. 119, No. 14, pp. 19-28, 2018

[9]. Sable Nilesh Popat*, Y. P. Singh," Efficient Research on the Relationship Standard Mining Calculations in Data Mining" in Journal of Advances in Science and Technology | Science & Technology, Vol. 14, Issue No. 2, September-2017, ISSN 2230-9659.

[10]. Sable Nilesh Popat*, Y. P. Singh," Analysis and Study on the Classifier Based Data Mining Methods" in Journal of Advances in Science and Technology | Science & Technology, Vol. 14, Issue No. 2, September-2017, ISSN 2230-9659.

[11]. DebaPraseadMozumder, Md. JulkarNayeenMahi, MdWhaiduzzaman, "Cloud Computing Security Breaches and Threats Analysis", International Journal of Scientific & Engineering Research, Vol. 8, Issue 1, pp. 1287-1297, 2017

[12]. YogachandranRahulamathavn, "Assessing Data Breach Risk in Cloud", International Conference on Cloud Computing Technology and Science (CloudCom), 2015, IEEE.