RESEARCH ARTICLE OPEN ACCESS

Security Enhancement in Cloud Computing Using Triple DES Encryption Algorithm

Tony Durgadas Jagyasi*, Jagdish Pimple**
*(Dept. of Computer Science and Engineering, Nagpur University, Nagpur, India
Email : jagyasitony@gmail.com)
** (Dept. of Computer Science and Engineering, Nagpur University, Nagpur, India
Email: pimplejagdish@gmail.com)

ABSTRACT
Cloud computing provides easy accessibility of the data from anywhere all the time. Due to the availability of the data over the cloud it is easy for every user to access the data. The user can also store the sensitive data so the security is the matter of concern of the sensitive data. So to provide security of the data, the database where all the user details (such as username, password, etc.) are available to access the data of the user is available in the encrypted form. So the owner of the cloud will also not be able to get inside the user space and will not be able to see the data of the user. With all this, the database and the data is available in the other cloud also as a backup of the main data, so that in case of failure of one cloud the user can get its data from other cloud.

***Keywords* -** Cloud Computing, Encryption, Triple DES, Cloud backup, Encryption Algorithm.

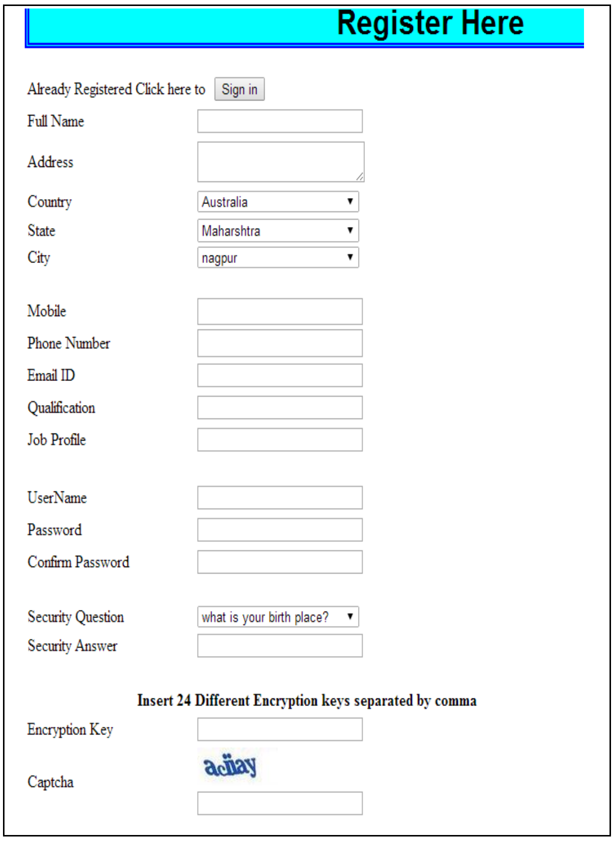
I. INTRODUCTION

The utilization of cloud computing has expanded quickly. Cloud computing gives numerous profits to the clients, for example, availability and accessibility. As the information is accessible over the cloud which is entered by number of distinctive clients, so there are some security issues. There may be touchy information of association which is stored over the cloud which might be accessed by any client. This is the one issue to give confirmation of the client to gain access to the information, even if it's the manager of the cloud or the top administration of the cloud.

The other issue could be if the cloud where the information is stored if fails. Assuming that such things happen then the information have to be stored in number of different cloud such as backup of the cloud, so if one cloud fails then the client will get the information from the other cloud. With this, the cloud will not get overloaded because of access of the same information by various confirmed clients.

II. Background And Related Works

The Triple DES algorithm will be used at the registration page where the user will need to register itself. The 3DES algorithm uses eight bytes per block. So the user will enter the different 24 bytes key to be used in the algorithm. The confidential 3DES key combined between the corresponding parties is appropriately 168-bits lengthy. This key comprises of 3 self-sufficient 56-bit numbers utilized by the DES algorithm. All of the 3 56- bit sub keys is placed as a 64-bit (8 octet) quantity, with the lowest possible significant bit of every octet used as a parity bit.



Register Here

Already Registered Click here to	Sign in
Full Name	
Address	
Country	Australia
State	Maharshtra
City	nagpur
Mobile	
Phone Number	
Email ID	
Qualification	
Job Profile	
UserName	
Password	
Confirm Password	
Security Question	what is your birth place?
Security Answer	

Insert 24 Different Encryption keys separated by comma

Encryption Key	
Captcha	

Fig. 1. Register page

As you can see in the above figure, the user will need to enter the 24 bytes key as needed by the

Triple DES algorithm. At this point the use of triple DES algorithm will be done.

The way the triple DES works is that the user needs to give three 56-bit keys, and encrypt with K1, decrypt with K2 and encrypt with K3. There are also 2-key and 3-key versions. In 2 key versions the user will define two different keys. As merely one where K1=K3. In 3-key versions there will be only 1-key i.e. if K1=K2=K3, then 3 DES is only Single DES.

Triple DES was created back when DES was getting a bit weaker than people were comfortable with. As a result, they wanted an easy way to get more strength. In a system dependent on DES, making a composite function out of multiple DES is likely to be easier than bolting in a new cipher and sidesteps the political issue of arguing that the new cipher is better than DES.

It would appear, when you create a figure into another one, you can't utilize a twofold enciphering. There is a class of assaults called meet-in-the-middle attacks, in which you scramble from one finish, decode from the other, and begin searching for crashes.

III. Methodology Used (Triple Des)

The 3DES encryption algorithm requires 3, 8 byte keys for encryption and decryption process. The user enters the key while registration for the cloud access i.e. when the user makes registration to access the cloud, the user has to choose the key which will be used as the key encryption and decryption of the user data. This will make the user to remember the key easily.

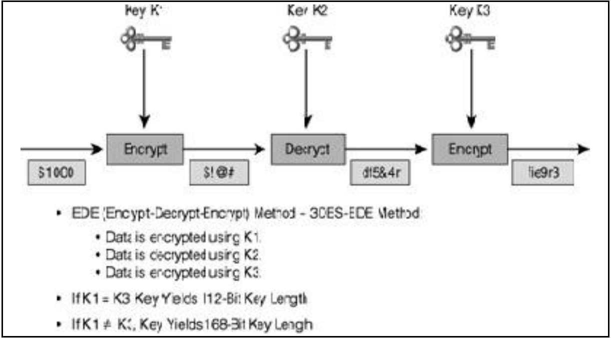

Key K1
Key K2
Key K3
Encrypt
Decrypt
Encrypt
$1000
$!@#
dt5&4r
ie9r3
EDE (Encrypt-Decrypt-Encrypt) Method - 3DES-EDE Method
Data is encrypted using K1.
Data is decrypted using K2.
Data is encrypted using K3.
If K1 = K3 Key Yields 112-Bit Key Length
If K1 ≠ K3, Key Yields 168-Bit Key Length

Fig. 2. Triple DES

The working of the triple DES is as follows:

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

Cipher text = EK3 (DK2 (EK1 (plaintext)))

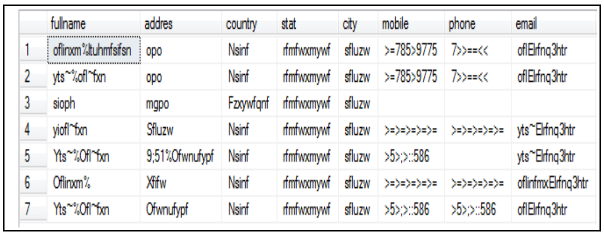
I.e., DES encrypts with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

Plaintext = DK1 (EK2 (DK3 (cipher text)))

I.e., decrypt with K3, encrypt with K2, and then decrypt with K1. [9]

While the user registers itself to access the cloud, the data will be maintained in the sql and the owner of the cloud will also not be able to see the data from the database as this data will also be available to the admin in the encrypted format as shown in the figure below.

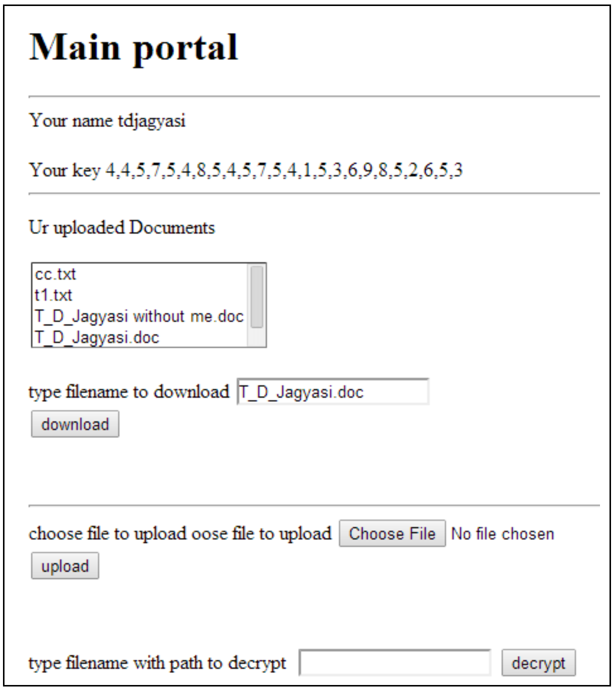


	fullname	addres	country	stat	city	mobile	phone	email
1	oflinxm%ltuhmfsifsn	opo	Nsinf	rfmfwxmywf	sfluzw	>=785>9775	7>>==<<	oflElrfnq3htr
2	yts~%ofl~fxn	opo	Nsinf	rfmfwxmywf	sfluzw	>=785>9775	7>>==<<	oflElrfnq3htr
3	sioph	mgpo	Fzxywfqnf	rfmfwxmywf	sfluzw			
4	yiofl~fxn	Sfluzw	Nsinf	rfmfwxmywf	sfluzw	>=>=>=>=>=	>=>=>=>=>=	yts~Elrfnq3htr
5	Yts~%Ofl~fxn	9;51%Ofwnufypf	Nsinf	rfmfwxmywf	sfluzw	>5>;>::586		yts~Elrfnq3htr
6	Oflinxm%	Xfifw	Nsinf	rfmfwxmywf	sfluzw	>=>=>=>=>=	>=>=>=>=>=	oflinfmxElrfnq3htr
7	Yts~%Ofl~fxn	Ofwnufypf	Nsinf	rfmfwxmywf	sfluzw	>5>;>::586	>5>;>::586	oflElrfnq3htr

Fig. 3. Database in Encrypted form

After completion of the registration for the cloud, the user has to activate its login i.e. a validation part by entering the code. After all these process are completed the user space will be created with the name of the user i.e. every user has to enter a unique username where all the files and other documents of the user are maintained.

After completing the validation part the user will be able to see the space created for the user where the user will enter the documents and its files are maintained securely. The user can see the complete list of files and folders user has created and maintained in its space as shown in the figure below.



Main portal

Your name tdjagyasi

Your key 4,4,5,7,5,4,8,5,4,5,7,5,4,1,5,3,6,9,8,5,2,6,5,3

Ur uploaded Documents

cc.txt
t1.txt
T_D_Jagyasi without me.doc
T_D_Jagyasi.doc

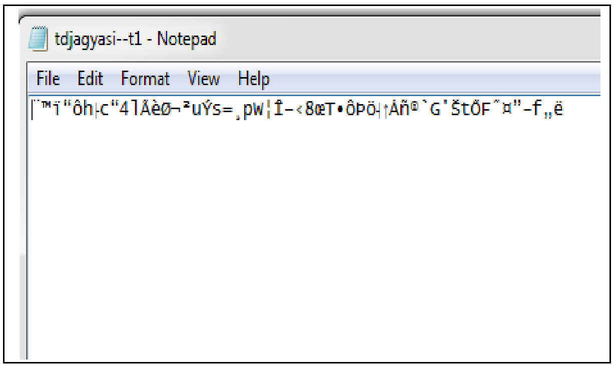
type filename to download T_D_Jagyasi.doc

choose file to upload oose file to upload Choose File No file chosen

type filename with path to decrypt

Fig. 4. User space/ Main page of the user

There is more security maintained while the user download its files from the cloud, the text and document files are downloaded but are available in the encrypted format, so if any unauthenticated user downloads the file of the user, it will get the files in encrypted form as can be seen in the figure below. While the aunthenticated user will known that after getting the files from the cloud it will have to be decrypted using the same key and encryption algorithm used by the user at the time of registration and the time of uploading the files.



```
¨™ï“ôh¦c“4]ÄèØ¬²uÝs=¸pW¦Î–‹8œT•ÔÞö¦†Åñ®`G'ŠtŐF˜¤"–f„ë
```

Fig. 5. Data in Encrypted form

Triple DES is an encryption and decryption algorithm which is used to encrypt the file and documents uploaded by the user. While the user is registering, the user is entering the 24 byte keys each of these are divided in 3 parts i.e. k1, k2, k3, which are used in the triple DES encryption algorithm. This algorithm is implemented in the main page of the user i.e. the page named main portal space of the user where user is maintaining its files. The result can be seen in the above figure.

IV. Conclusion

The user will register and will get the cloud space. While registering the user has given the key which will be used as encrypted and decrypted purpose. As the user will register its space will be created and after validating the account the user can store the files and documents in the encrypted form.

V. Future Work

At this part, the user is able to upload all the files and can maintain the security of the data. In the future, the user will also be able to upload images and videos in its space. This will also be encrypted using the encryption algorithm so that the authentication of the cloud user will be maintained and security of the files and images will be done.

References

[1] Privacy Preserving Public Auditing for secure cloud storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE.

[2] Insider Threats to Cloud Computing: Directions for New Research Challenges BY William R Claycomb, Alex Nicoll Carnegie Mellon University.

[3] Efficient Computing With Cloud. Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[4] Cloud Computing Security: From Single to Multi-Clouds 2012 45th Hawaii International Conference on System Sciences.

[5] Impact of Cloud Computing on IT Industry: A Review & Analysis International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 01– Issue 02, November 2012.

[6] DES, AES, Blowfish: symmetric key cryptography algorithm simulation based performance analysis International Journal of emerging technology and advanced engineering.

[7] Superiority of blow fish. International Journal of Computer Application Volume 2 No 9 September 2012.

[8] Comparison between DES, 3DES, RC2, Blowfish and AES Milind Mathur and Ayush Kesarwani.

[9] http://en.wikipedia.org/wiki/Triple_DES.

[10] http://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained