International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Key-Aggregate Cryptosystem for Scalable Data Sharing In Cloud Storage

Paga Bhavana , Mamidala Sagar, Dr.A.Satyanaraya
H.T.NO: 15TQ1D5808,
[1]Pursuing M.Tech (CSE), Siddhartha Institute of Technology and Sciences, Hyderabad.
[2]Assistant professor, Siddhartha Institute of Technology and Sciences, Hyderabad.
[3]Associate professor, Siddhartha Institute of Technology and Sciences, Hyderabad

ABSTRACT:

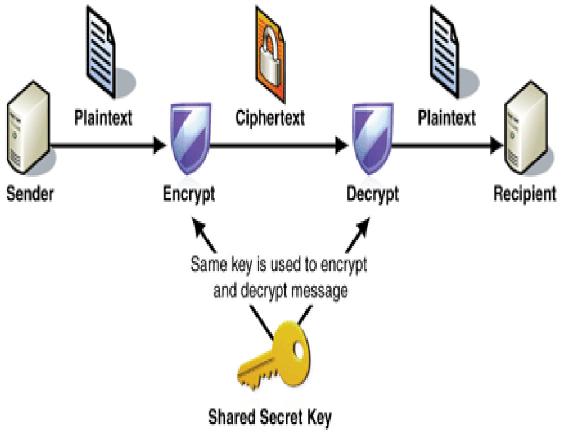
But in now a day's all cloud computing applications so many data privacy problems are raised. So many data privacy issues are in cloud computing. These data privacy issues are overcome by provide authentication for users and server. If any unexpected privileges to users it occurs some data loss problems. These data privacy issues are occurred in group shared data applications in cloud computing environment. In group data sharing applications different virtual machines are assigned to different clients and all clients are connected to single physical machine. In this scenario providing confidentiality and privacy to shared data in different customers. In this applications using cryptographic techniques to provide security for data.

In cloud computing data sharing functionality is very important. Data owners upload data in cloud server. In normal existing systems directly store original data but third party hackers hack the data and modify the data eaves droppers and tampering attacks are very high in cloud applications. So that's why in present cloud data share applications using encryption and decryption techniques provide security for data. Data owners upload data in cloud server before uploading the data is encrypted by using any cryptographic algorithm and stored in cloud server. If customers want to download data in that data owners share private key to particular customers. Based on private key customers decrypt the data and download original readable format of data from cloud server.

1. EXISTING SYSTEM

Symmetric encryption

In case of symmetric encryption, for example Alice want to share information to bob. By using public key encrypt the data and send to bob. Bob want to decrypt the data by using same public key get original data from Alice. Only single same key is used in encryption and decryption it is not provide more security for data in cloud server. Following diagram shows the symmetric encryption procedure.



Architecture of symmetric encryption

Describes the symmetric encryption mechanism in which sender encrypts the data with a public key and send the public key to the receiver by which receiver decrypt the encrypted data with same public key.

Asymmetric encryption

In asymmetric encryption by using public key cryptosystems provide more security because of in public key crypto systems using different keys to encrypt and decrypt the data. In cloud data sharing applications public key cryptosystems gives more flexibility and efficiency then compared to symmetric encryption techniques. In this public key cryptosystems Alice want to send data using public key and encrypt and send to bob. In receiver side bob want to decrypt the data by using bob's secret key decrypt the data. In this using two keys public key and secret key. Public key is common for sender and receiver. But private keys are different from sender and receiver.

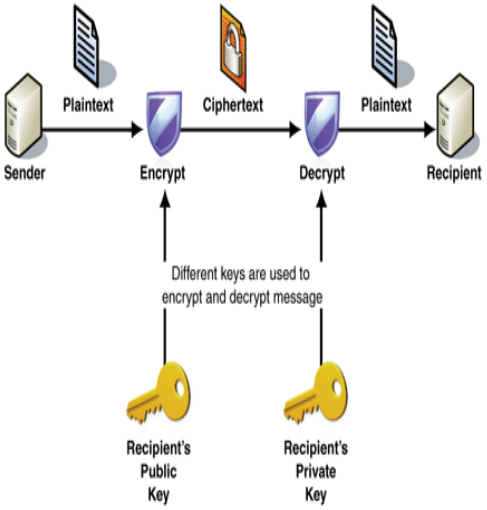


Figure 1: Architecture of asymmetric encryption

Figure 2 describes the asymmetric encryption mechanism. In which sender encrypt the data with recipient's public key and send to the receiver. Then receiver decrypts the encrypted data with his/her own private key.

In present system, symmetric cryptographic techniques are used to encrypt and decrypt the data by using a single key. But it doesn't provide more security for data. Then compared to symmetric techniques asymmetric techniques provide more security by using different keys and encrypt and decrypt the data. So here discuss about how to implement new cryptographic technique to provide more security for data cloud server. Encryption is one by one key and decryption is done by another different secret key in cryptography.

2. PROPOSED SYSTEM

The problem is solved by introducing a special type of public-key encryption which is called as key-aggregate cryptosystem (KAC). In this proposed system generally admin upload files into server in encryption format. Customer wants to download file from server using secret key or aggregate key and downloaded file in decrypt format.

3. FUNCTIONALSPECIFICATIONS

1 SETUP PHASE

There is no input for setup algorithm except security implicit parameter. The of the setup page output is a master key MK. public parameters PK and

2 ENCRYPT PHASE

Encrypt (PK, M, A). The public parameters PK is input for encrypt phase

3 KEY GEN PHASE

Key Generation (MK, S). Master key MK is input for algorithm of key generation and a set of attributes S that describe the key

4 DECRYPT PHASE

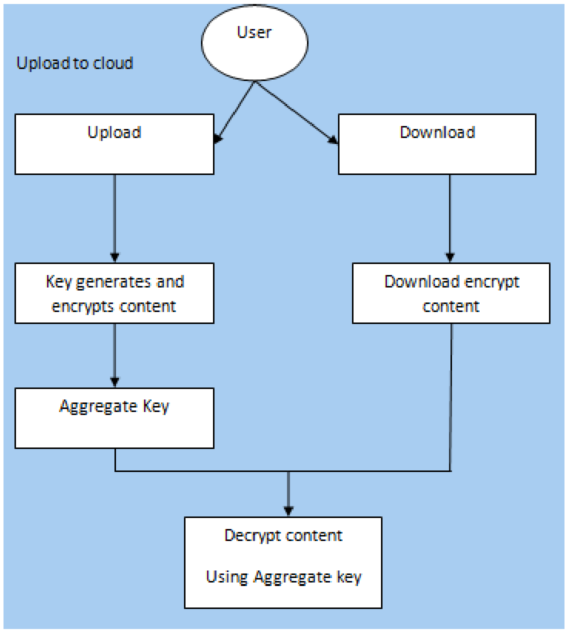
Decrypt (PK, CT, SK). The decryption algorithm takes as input the public parameters PK, a cipher text CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes.

Sharing Encrypted Data

Data sharing in key aggregate crypto systems is efficient and flexible. In this schema sharing the data from one user to another user in confidential manner with variable and small cipher texts format.

Data sharing in key aggregate crypto systems

Describes that, Alice encrypt all her data and stores in cloud. Bob need some of Alice's data, and send request to Alice for particular data. Bob's requested data is present in 2, 3, 5 class indexes. So, Alice generates an aggregate key of 2, 3, 5 and send the single aggregate key to Bob. By using the single aggregate key Bob download and decrypt the data.



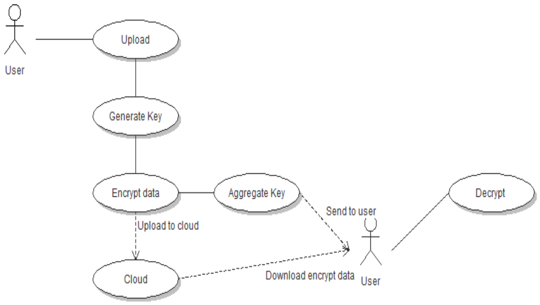
Architecture of key aggregate method

Describes the design of key aggregate method. This model contains two scenarios, one is to upload the data and transfer to other user, and other is to download the data.

If user wants to upload the data generates the keys and encrypt the using those keys and generates a single aggregate key and sends it to other user. If user wants to download the data, he/she downloads the data and decrypts the encrypted data using the aggregate key.

Use case diagram:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis.

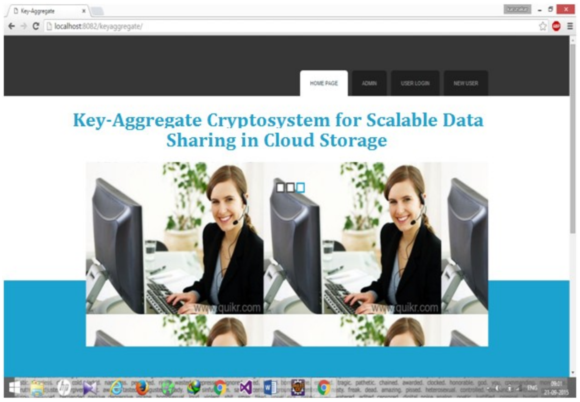


Activity diagram

Describes the project flow and what are activities performed in project and Activity diagram for user

4.RESULTS:

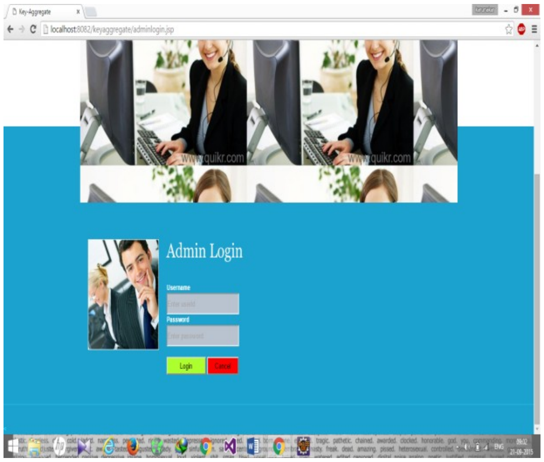
The experimental results will have the screen shots of the project when executed. The front page of the project when no input is given; just the starting page of this project is as follows.



Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage

Screen of Home page

User click on admin tab display the admin login form



Input:

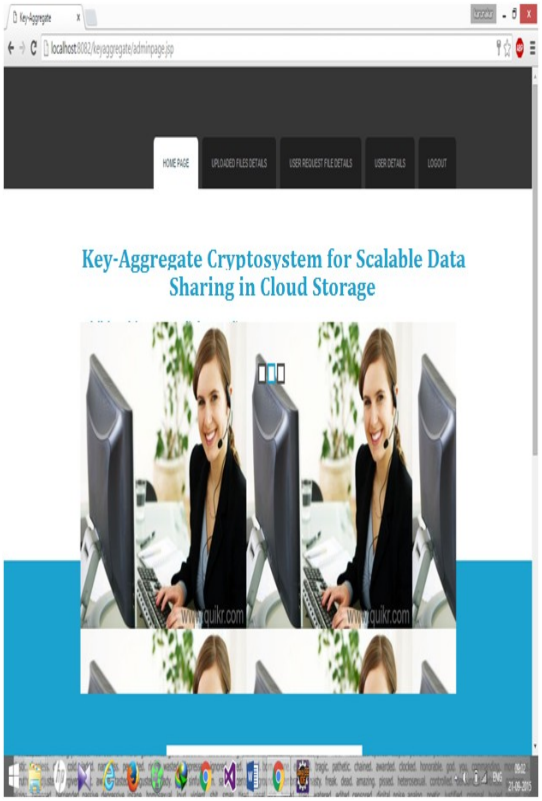
Admin enters all details and click on login button

Description:

When clicks on login button check all validations. If enter correct details display admin home page

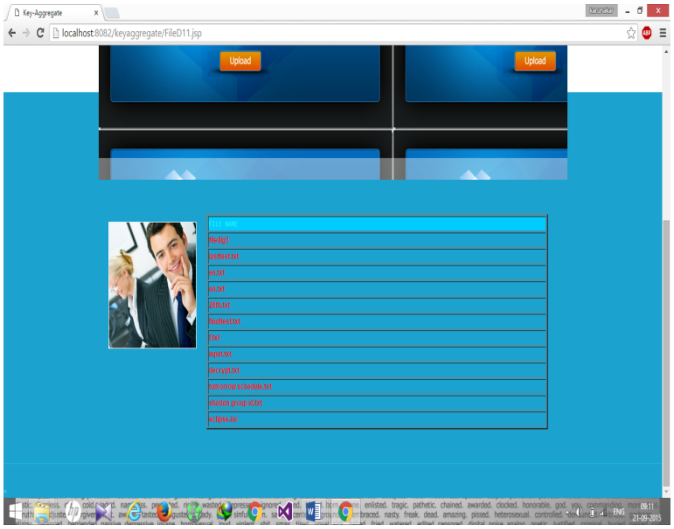
Output:

Verify admin details if he is valid display admin home page form


Key-Aggregate
localhost:8082/keyaggregate/adminpage.jsp
HOME PAGE
UPLOADED FILES DETAILS
USER REQUEST FILE DETAILS
USER DETAILS
LOGOUT
Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage

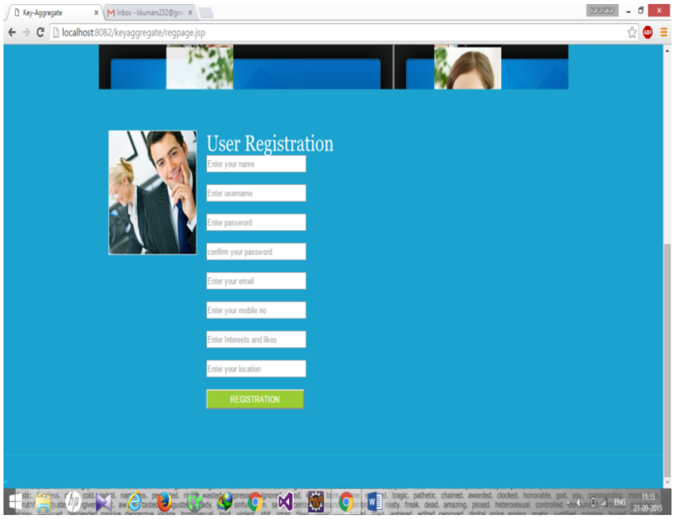
Screen of Admin's home page

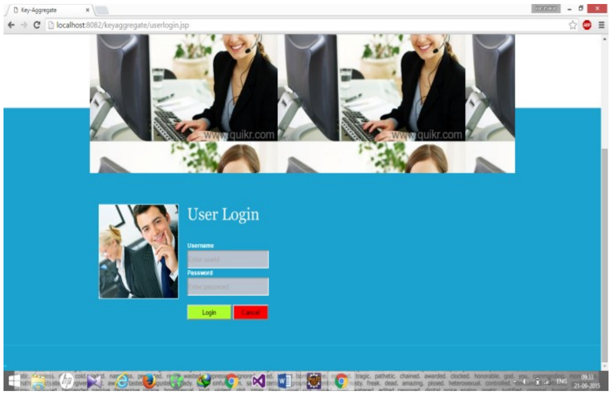
The Admin’s home page, which consists of operations have to be performed by Admin.



FILE NAME
filedig3
lasttest.txt
en.txt
en.txt
28th.txt
finaltest.txt
f.txt
input.txt
decrypt.txt
tomorrow schedule.txt
shadan group id.txt
eclipse.ini

Screen of Admin's uploaded files details





Screen of User's login page

Input:

User enters all details and click on login button

Screen of new user page

The new user page, which consists of the registration

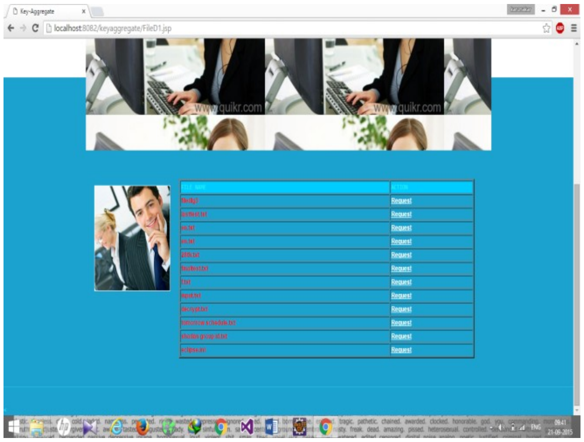
Description:

When clicks on login button check all validations. If enter correct details display user home page

Output:

Verify user details if he/she is valid display user home page form

The above screen (Figure 27) shows the user's home page, which consists of operations have to be performed by user.



FILE NAME	ACTION
file-dig3	Request
lucifiest.txt	Request
en.txt	Request
en.txt	Request
200r.txt	Request
finaltest.txt	Request
f.txt	Request
input.txt	Request
decrypt.txt	Request
tomorrow schedule.txt	Request
shadan group id.txt	Request
eclipse.ini	Request

Screen of request for files for every file by which user can request for particular file.

5. CONCLUSION

This approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.

Finally conclude that in this type of sector data sharing applications using encryption and decryption technique provides more security. By using this type of key aggregate generation and verification algorithms improve system performance and efficiency.

6. REFERENCES:

[1] Myungho Lee, Jin-hong Jeon*, Joonsuk Kim, Joonhyun Song. "Scalable and Parallel Implementation of a Financial Application on a GPU: with focus on out-of-core case." In proceedings of the 10th IEEE International Conference on Computer and Information Technology, Pages 1323-1327(2010).

[2] Mike Roney, Vice President, Investments The Roney Group of Raymond James & Associates, Inc. march, 2009.

[3] Barry R. Cobb,John M. Charnes. "Approximating free exercise boundaries for American-style options using simulation and optimization." In Proceedings of the 2004 Winter Simulation Conference, Pages 1231-1238.