Key exchange privacy preserving technique in cloud computing

Pooja Bandal[1], Ashwini Dhane[2], Shubham Chavan[3], Prof. Nilima Nikam[4]

[1,2,3] Students, Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering and Technology, Maharashtra, India
[4]Professor, Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering and Technology, Maharashtra, India

---***---

Abstract- *Today's IT world uses cloud in very huge amount which is flexible storage to store users document or files .Cloud is cost efficient and time efficient method to store data. Because of this, some security issues are occurred in the cloud hence cloud security is the main problem in cloud computing. Even if many companies are gives security to cloud the user are not satisfied by the security facility of the cloud. So in our project we use a key exchange algorithm i.e Diffie Hellman to store data securely by sharing the secret keys between the users so they can upload or download files in the cloud. This is efficient way technique for preserving the privacy of cloud.*

Index Terms – Privacy, protocols, cloud computing, DH(Diffie Hellman algorithm) etc.

1) INTRODUCTION

Cloud is the most efficient storage for the users.so the cloud computing is popular topic becomes in technical world. Privacy preserving of cloud is become a major issue so the data in the cloud should be stored in encrypted form. After encryption of the data sometimes data will be leaked and even if it's not this method is cost and time consuming .

Hence this is not most efficient way of preserving the data Even if the security of data maintained the information of users are not stored securely hence there is might be chance to suspicious person can access the documents in the cloud. To restrict client from accessing the shared data directly, proxy and brokerage services should be employed, still leakage of data has become greater issue in cloud computing so we created simple application on the Netbeans which gives authentication in cloud using login facility so can only specified user can log in .Here we use cloud as a server which store the files. For storing the file we use aws services which can use to upload and download files. To give security to user data(cloud storage)we use key exchange algorithm.

1.1 LITERATURE SURVEY

T. Shu, Y. Chen, J. Yang, and A. Williams- 2014 -"Multilateral privacy-preserving localization in pervasive environments"- They both suggested that novel privacy-preserving optimization framework for participatory sensing. This framework allows the two parties of the sensing, i.e., the This framework allows the two parties of the sensing, i.e., the Platform and the mobile users, to share data for the formulation of the optimization, but without revealing sensitive information that may lead to the privacy leakage of each other.

Ye Yan, Dong Han, and Tao Shu- 2016-Privacy Preserving Optimization of Participatory Sensing in Mobile Cloud Computing" - In this they has suggested only find out which is the efficient way for security of the cloud. They find out efficient process by using matlab.

Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy -2010- "Token-Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency"- In this they used homomorphic token security technique which is not that much provide security to user data in the cloud.

Jian Shen, Dengzhi Liu, Jun Shen, Haowen Tan, Debiao He- 2015-"Privacy Preserving Search Schemes over Encrypted Cloud Data"- It is a Comparative Survey. which only took search for privacy preserving problem issues and need of security in the cloud computing.

1.2 COMPARATIVE ANALYSIS

Title	Year of published	Technique used	Alogorithm	Demerits
Token-Based Cloud Computing Secure Outsourcing of Data	2010	Homo-morphic token .	Homomorphic token generation algorithm	Not efficient method of data security
Multilateral privacy-preserving localization in pervasive environment.	2014	No security only optimization techniques used	-	No security to data

Privacy Preserving Optimization of Participatory Sensing in Mobile Cloud Computing	2016	The techniques are only analysed	Matlab used to find out efficient method of security	Only analysing done no practical solution was found.
Privacy Preserving Search Schemes over Encrypted Cloud Data: A Comparative Survey	2015	-	-	Survey done without find out the best solution.

2) EXISTING SYSTEM

Cloud is a huge storage facility for the users so they uses it on very huge amount. The data is also stored in large amount.

The companies are giving priority to how to data can be optimized .hence the security got the least priority. As the cloud used by the people in large scale so there might have chances to leak the data.

Solution of that problems getting in very ways but authentication and security problems is still rapidly increasing.
Even if data is in encrypted form the preservation of data is not possible because hacker can easily hack the data.

Even if the companies provides security to cloud the data can be hacked because existing system uses the homogenous key exchange privacy where key can easily be leaked .

3) PROBLEM DEFINATION

1) Confidentiality in the cloud computing using encryption methods (like Full Disk Encryption) that encrypt stored data on hard disk throughout the booting process. Whole Disk Encryption is also used for encrypting the data with the well-known AES (Advanced Encryption Standard) algorithm. If the device that is using cloud computing technology is lost or stolen the whole information will be lost.

2) Because clouds are massive in scale compared with private data centers, they're much bigger targets for hackers .By using homogenous key algorithm the data is stored whereas even if it is time efficient method the key can be easily hacked, so data prevention is difficult for companies.

3) Token Based Cloud Computing Secure Outsourcing of Data in which token will be formed to secure the data but it form homomorphic tokens which can be easily hacked.

We are using key exchange algorithm called diffie hellman algorithm. This algorithm takes to prime no to form their mod function and form it as a secret key.

When user want to share or store some data the two keys are (prime no's) generated by our application and the secret key will form and stored in cloud database .database have its own secret key when user want to interact with cloud it just simply login in cloud for authentication and then the both the users and database keys are exchanged and verified if they are matched the file will be download or upload. Otherwise it cannot access the cloud.so no another user can hacked the data so data will be preserved.

4) PROPOSED SYSTEM

The application have the login facility so the authenticated user can be login in the cloud .Also the information about the users are also stored for further process of sharing or storing the database. To store the data and information the Amazon cloud is used.

Amazon cloud has AWS (amazon web service) which is used for database service and storage service.

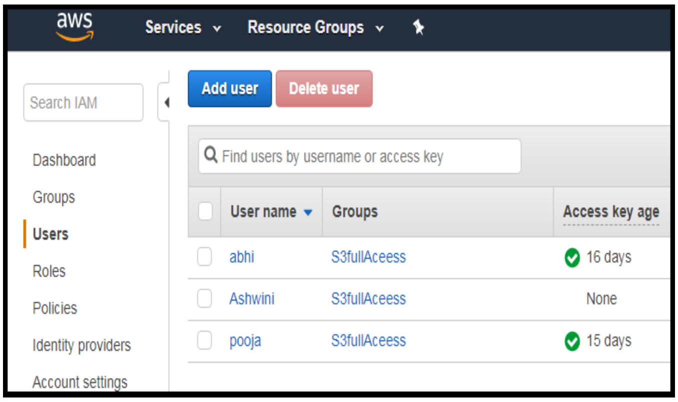
The following two services are used from the aws

1) S3(simple storage service)
2) RDS(relational database service)

- **S3(simple storage service)**

Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web.

To store the user confidential information we used S3 service from the cloud. After login in our application user have the choice to store or download the file.



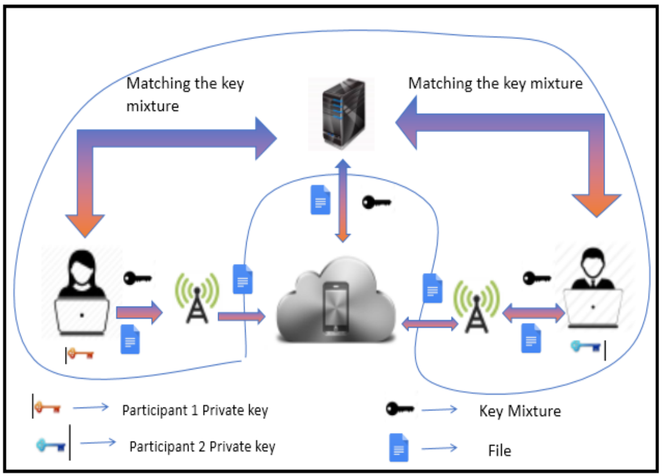
User name	Groups	Access key age
abhi	S3fullAceess	✓ 16 days
Ashwini	S3fullAceess	None
pooja	S3fullAceess	✓ 15 days

- **RDS(relational database service)**

Relational database service is used for to store the user information.

So all details of users will be stored hence if any suspicious person login in cloud can be easily found out.

Also for Diffie-Hellman key exchange algorithm the secret key is formed that key is also stored on the database.



System Architecture

Advantages:

1) The Data is fully secured and transferred without any leakage of sensitive information of any participants.

2) The Data Privacy is preserved with the help of Diffie-hellman key exchange protocol.

5) ALGORITHM USED

1) First user must have to login or sign up on the application.

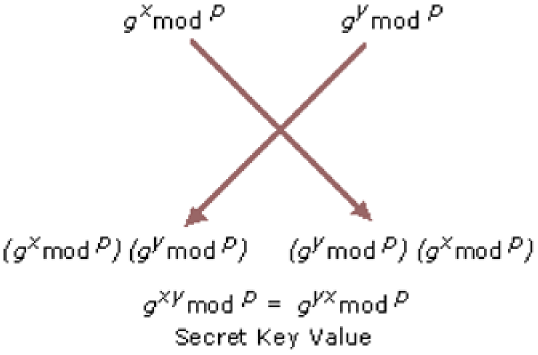
2) Then created the secret key for the database for security maintenance for the files using diffie- hellman.

3) After successfully login, the two keys are generated(two prime numbers).The mod function of that numbers is find out & that number is assigned to secret key and stored in database with the user information.

4) Then the key exchanged algorithm is applied between the database secret key and user's secret key

The Diffie hellman security algorithm system as follows-

1. Database and user agree on a prime number, p, and a base, g, in advance.
2. User1 chooses a secret integer number and computes A = g^a mod p.
3. User chooses a secret integer b and computes B = g^b mod p.
4. Database sends A to user and user sends B to Database.
5. To obtain the shared secret, Database computes s = B^a mod p.
6. To obtain the shared secret, user computes s = A^b mod p.


g^x mod p
g^y mod p
(g^x mod p) (g^y mod p)
(g^y mod p) (g^x mod p)
g^{xy} mod p = g^{yx} mod p
Secret Key Value

After applying the Diffie-hellman if the keys are matched then and then only user have facility to upload and download file .then after uploading the file the file will be visible in the cloud and also can see file list stored in cloud.

6) IMPLEMENTATION DETAILS

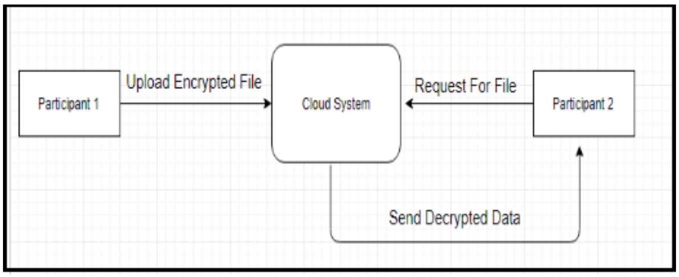
In this project. we used Hard Disk of 20GB and Above, RAM used is 256 MB and We used Processor of 1.6 GHz . We used front end as a java (netbeans), and AWS cloud in back end. In AWS cloud we used 2 services RDS(Relational database) and S3 (simple storage service).

In Our project we used RDS for storing users information and key information while in S3 service stores users data that means we create bucket for uploading and downloading the files.

First of all we created login application in netbeans by using java where we create keys in sign-up process and those keys are saved in RDS database. This database is also used for authentication process. Now only authenticated user can access their account. So the users can upload and download the files through the application. To make the security stronger we used Diffie Hellman key exchange algorithm to verify users each time while user uploading or downloading the files.

In While signing up a random prime number is generated which will be kept as private key and another public key will be calculated which will be a public key to exchange. In the same way public and private keys are created for database side which will be used to verify the user in further process.

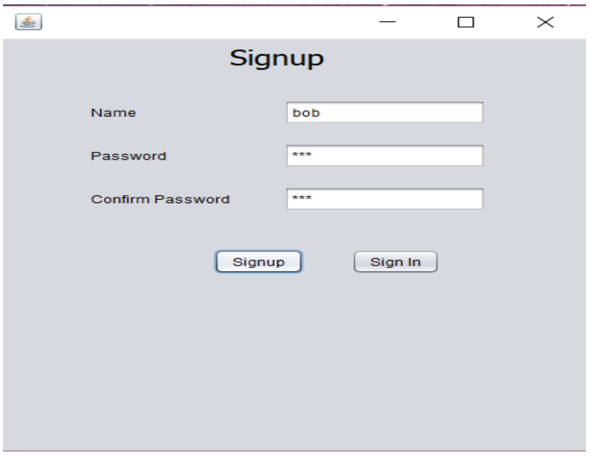
When user wants to download or upload the file he will first get verified with Diffie Hellman algorithm. Here the public key of the user will be send for verification which will be retrieved from RDS with public key of database. Using the formulas of Diffie Hellman common key calculated. If the calculated key is same then further process of uploading and downloading will process else the process for the user will the denied. In this way the security for the cloud is maintained.



7) RESULT ANALYSIS

1) First user successfully signed up on cloud.When the user will successfully login on the page the application create two prime numbers for the further process.

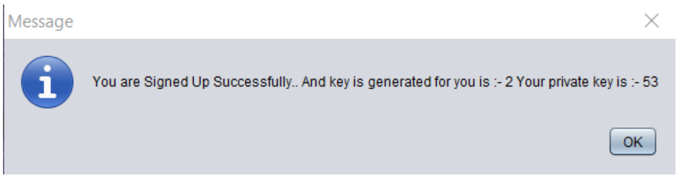
Following shows the sign up and login page


Signup

Name bob

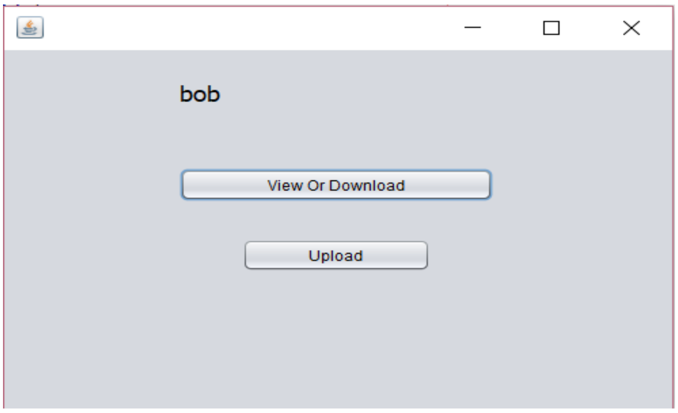
Password ***

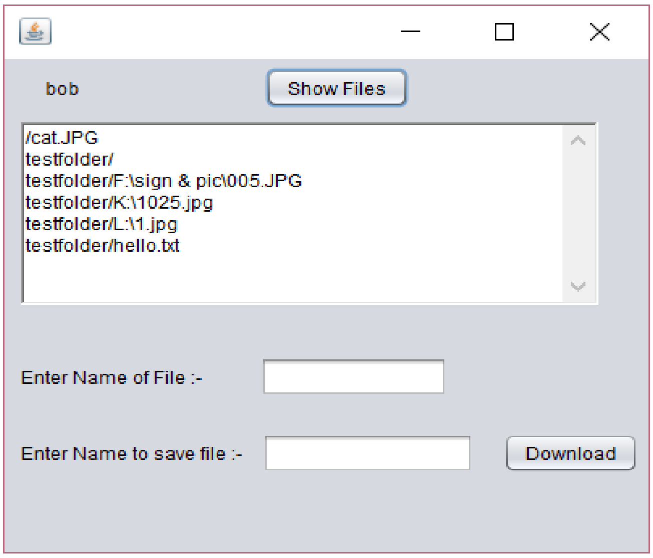
Confirm Password ***


Message

You are Signed Up Successfully.. And key is generated for you is :- 2 Your private key is :- 53

2) After successfully login the downloading or uploading option will appear. After that showing files in the cloud while the user choose the option download the file.


bob


bob

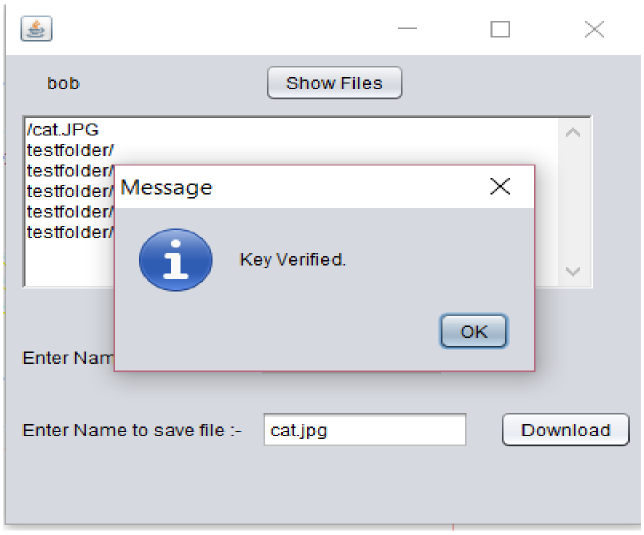
/cat.JPG
testfolder/
testfolder/F:\sign & pic\005.JPG
testfolder/K:\1025.jpg
testfolder/L:\1.jpg
testfolder/hello.txt

Enter Name of File :-

Enter Name to save file :-

3) Then the keys are verified which are secret keys formed by the mod functions using two prime numbers.

The successful key verification shown as follows


bob

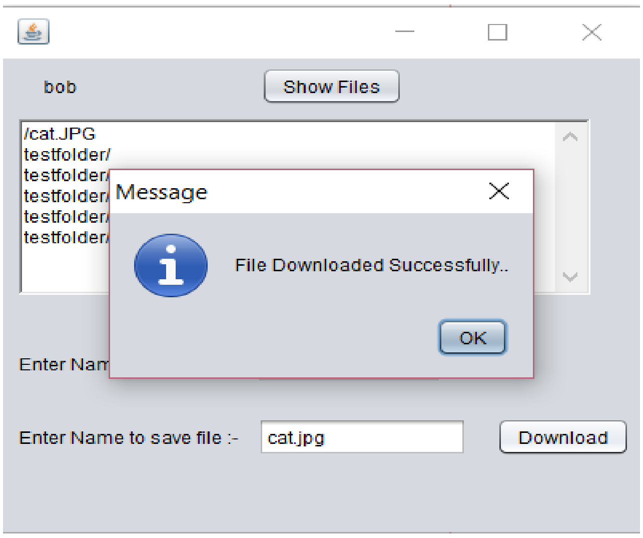
/cat.JPG
testfolder/
testfolder/
testfolder/
testfolder/
testfolder/

Message

Key Verified.

Enter Nam

Enter Name to save file :- cat.jpg


bob

/cat.JPG
testfolder/
testfolder/
testfolder/
testfolder/
testfolder/

Message

File Downloaded Successfully..

Enter Nam

Enter Name to save file :- cat.jpg

8 Conclusion

We proposed a privacy-preserving efficient framework based on Diffie Hellman message exchange protocol which provides Certain privacy guarantee to users in the cloud and also sign up facility for the user to communicate in the cloud. We successfully create key exchange facility to aws cloud using simply sharing secret key between the users . No one can see or share the data only authenticated user can upload or download files in the cloud.

REFERENCES:

1) T. Shu, Y. Chen, J. Yang, and A. Williams, "Multi-lateral privacy-preserving localization in pervasive environments," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 2319–2327.

2) J. Vaidya, "Privacy-preserving linear programming," in Proceedings of the 2009 ACM symposium on Applied Computing. ACM, 2009, pp. 2002–2007.

3) Ye Yan, Dong Han, and Tao Shu,"Privacy Preserving Optimization of Participatory Sensing in Mobile Cloud Computing" in 2016- IEEE 37th International Conference on Distributed Computing Systems

4) 4) Jian Shen, Dengzhi Liu, Jun Shen, Haowen Tan, Debiao He, "Privacy Preserving Search Schemes over Encrypted Cloud Data: A Comparative Survey", Computational Intelligence Theory Systems and Applications (CCITSA) 2015 First International Conference on, pp. 197-202, 2015.