Securing and Compressing Data in Clouds

Prof. A. V. Yenkikar[1] Nikhil Pandit[2] Shrikant Shinde[3] Prof.A.S.Mane[4] Sachin Rajage[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]DCOER, Pune

Abstract— Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users The aim is to secure the data stored on the clouds. For this, the document uploaded on the cloud by the server is encrypted. The client on the other side downloads the document and decrypts it in order to view the contents. Thus, in cloud computing environment there are many cloud servers, so the data will not be secured due to unreliable network communications. This problem can be eliminated by RSA algorithm.

Key words: RSA algorithm, Cloud computing

I. INTRODUCTION

The cloud services mainly include sharing of data, storage, Web-based email and database processing. By adapting the Cloud computing [1][3], it becomes very simple to share the resources. Users need not to worry about any knowledge of the services and it's very easy to maintain when compared to any traditional technologies. Cloud computing is of three types named Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS) .By these three, it is possible to make complex things very easy. Infrastructure as a Service (IaaS)[2] delivers basic storage and computing capabilities as standardized services over the network.

A. User Classes and Characteristics:

Anyone can use this system as it is simple. There is also an cloud agent who will monitor the system.

B. Operating Environment:

The computer used for browsing must have windows operating system installed on it. It must have internet connection for retrieving the data from cloud.

C. Design and Implementation Constraint:

Design of the project is user friendly so that it can be used by anyone.

D. Assumptions and Dependencies:

The Cloud server we are using must be active. The users must have internet connection and windows operating system installed on their computers.

E. Drawbacks of the Existing System:

In Existing System, the data stored on cloud is not encrypted at owner's PC. The document gets directly uploaded on the cloud where it gets encrypted. In this case there is no guarantee of security of data.

F. Literature Survey:

1) DES/3DES or TripleDES:

This is an encryption algorithm called Data Encryption Standard that was first used by the U.S. Government in the late 70's. It is commonly used in ATM machines (to encrypt PINs) and is utilized in UNIX password encryption. Triple DES or 3DES has replaced the older versions as a more secure method of encryption, as it encrypts data three times and uses a different key for at least one of the versions.

2) Blowfish:

Blowfish is a symmetric block cipher that is unpatented and free to use. It was developed by Bruce Schneier and introduced in 1993.

3) AES:

Advanced Encryption Standard or Rijndael; it uses the Rijndael block cipher approved by the National Institute of Standards and Technology (NIST). AES was originated by cryptographers Joan Daemen and Vincent Rijmen and replaced DES as the U.S.Government encryption technique in 2000.

4) Twofish:

Twofish is a block cipher designed by Counterpane Labs. It was one of the five Advanced Encryption Standard (AES) finalists and is unpatented and open source.

5) IDEA:

This encryption algorithm was used in Pretty Good Privacy (PGP) Version 2 and is an optional algorithm in OpenPGP. IDEA features 64–bit blocks with a 128–bit key.

6) MD5:

MD5 was developed by Professor Ronald Riverst and was used to create digital signatures. It is a one–way hash function and intended for 32–bit machines. It replaced the MD4 algorithm.

7) SHA–1:

SHA–1 is a hashing algorithm similar to MD5, yet SHA–1 may replace MD5 since it offers more security.

8) HMAC:

This is a hashing method similar to MD5 and SHA–1, sometimes referred to as HMAC–MD5 and HMAC–SHA1.

9) RSA Security:

1) RC4– RC4 is a variable key–size stream cipher based on the use of a random permutation.
2) RC5– This is a parameterized algorithm with a variable block, key size and number of rounds.
3) RC6– This an evolution of RC5, it is also a parameterized algorithm that has variable block, key and a number of rounds. This algorithm has integer multiplication and 4–bit working registers.

II. ENCRYPTION AND DECRYPTION PROCESS

In Proposed system, the data is encrypted using RSA algorithm and then the data is uploading on the cloud.
At client's PC client needs to decrypt the document in order to view the document. To compress the data in order to save the space on cloud. To maintain data integrity. To maintain data privacy by using RSA.

RSA algorithms get executed in Polynomial time and other actions like data uploading and downloading also get completed in Polynomial time.

All rights reserved by *www.ijsrd.com*

Hence this system gets executed in Polynomial time.So our system is P-type system.

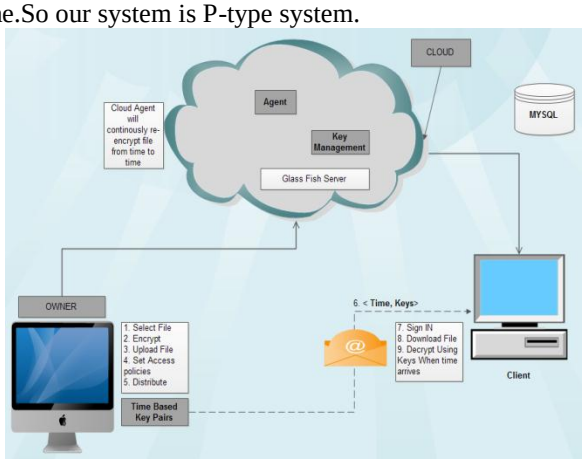


Fig. 1: Encrytion and Decryption and process

A. System Works As Follows:

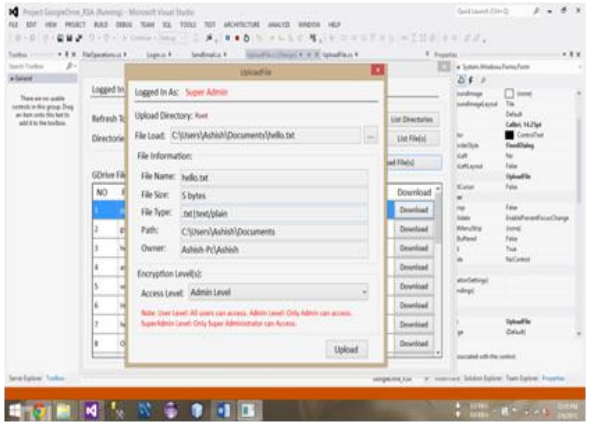
1) Step 1- selects the file.
2) Step 2- encrypt and upload the file.
3) Step 3- generate and distribute decryption key.
4) Step 4- sign in and download the document.
5) Step 5- decrypt the document in order to view the content of document.
6) step6- logout and close

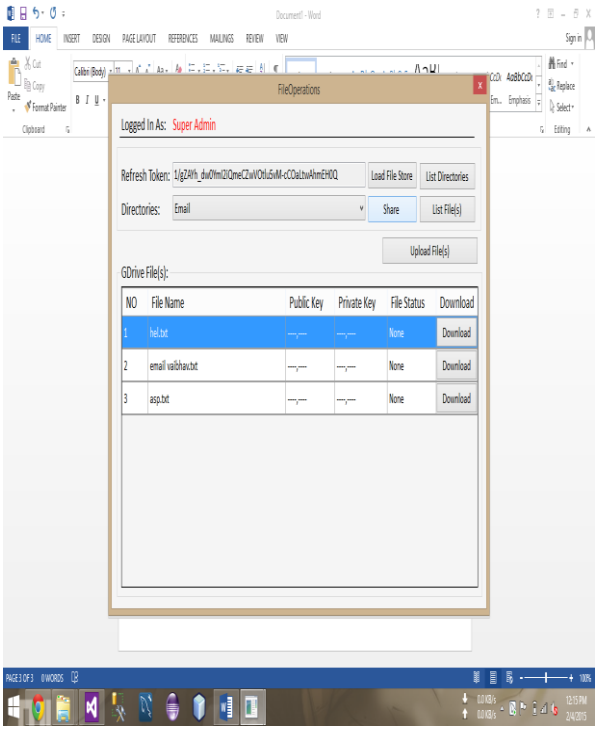
III. ALGORITHM

A. Working of RSA Algorithm:

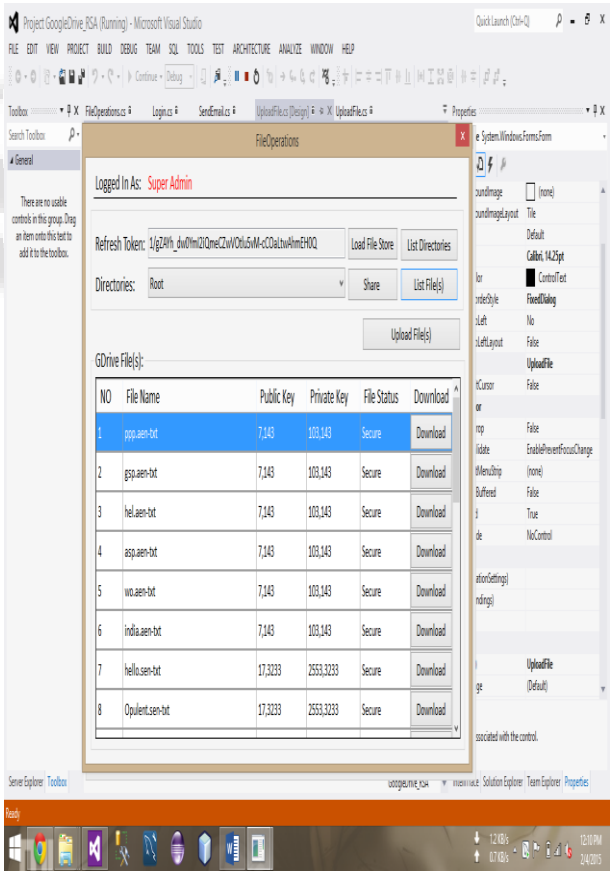
1) Step 1: Start
2) Step 2: Choose two prime numbers
   p = 3 and q = 11
3) Step 3: Compute the value for 'n'
   n = RSA.n_value (RSA_P, RSA_Q);
   n = p * q = 3 * 11 = 33
4) Step 4: Compute the value for? (n)
   ? (n) = (p - 1) * (q -1) = 2 * 10 = 20
   Int phi = RSA.cal_phi (RSA_P, RSA_Q);
5) Step 5: Choose e such that 1 < e <? (n) and e and nare coprime. Let e = 7
   Step 6: Compute a value for d such that (d * e) %? (n) = 1. d = 3
   Public key is (e, n) => (7, 33)
   Private Key is (d, n) => (3, 33)
6) Step 7: Stop.

IV. LOGIN DETAILS





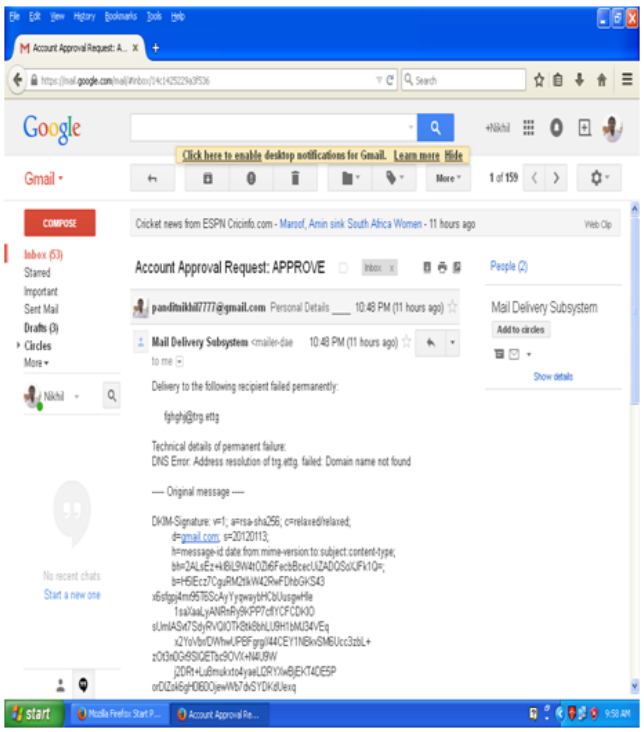
V. SENDING DECRYPTION KEY



logged information is shown on dashboard.set roll of user as super admin .dashboard shows google drive setting, load the user information. fill information i.e. user id, password, roll. change the status as approved or disapproved. if user is approved the system send mail to user as status is approved.

All rights reserved by *www.ijsrd.com*

VI. REQUEST APPROVAL MESSAGE



The approval mail is sent to the user after admin changed the status of user as approved..

VII. CONCLUSION

In this paper multiple access levels for the document can be added in order to make it more secure .In this paper more security can be provided to the important documents using RSA Algorithm.

REFERENCES

[1] J.H. Yeh, "A PASS scheme in cloud computing protecting data privacy by authentication," International Symposium on Biometrics and Security Technologies, 2013

[2] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012.

[3] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," Communications of the ACM, 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine grained data access control in cloud computing," in Proc. of IEE INFOCOM, 2010.

[5] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. Of ACM CCS (Poster), 2010.

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption withefficient revocation," in Proc. of ACM CCS, 2008.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. of IEEE Symposium on S&P, 2007.

[8] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and proxy cryptography," Advances in Cryptology–EUROCRYPT, 1998.

All rights reserved by *www.ijsrd.com*