RESEARCH ARTICLE OPEN ACCESS

Data Encryption in Unreliable Clouds

Prof. Anuradha Yenkikar, Nikhil Pandit, Shrikant Shinde,
Omprakash Pawar, Sachin Rajage
Department of Computer Science and Engineering
ZES's Dnyanganga College of Engineering and Research
Pune
Maharashtra - India

ABSTRACT
The aim is to secure the data stored on the third party. For this, the document uploaded on the cloud by the server is encrypted. The client on the other side needs to download the document and decrypt it in order to view the contents. Thus, in cloud computing environment there are many cloud servers, so the data will be not secured due to unreliable network communications. This problem can be solved by RSA algorithm.
Keywords:- RSA algorithm, Encryption, Decryption

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 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.

1.1. Project Scope

- Registration of users
- Encryption of information using RSA
- Uploading the data on the cloud.
- Decrypting the data at other end

1.2. User Classes and characteristics:

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

1.3. 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.

1.4. Design and Implementation Constraint

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

1.5. 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.

1.6. 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.

1.7. Proposed System

- In Proposed system, the data is encrypted using RSA algorithm and then the data is upload 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.
- Hence this system gets executed in Polynomial time.
- So our system is P-type system.

II. ARCHITECTURE

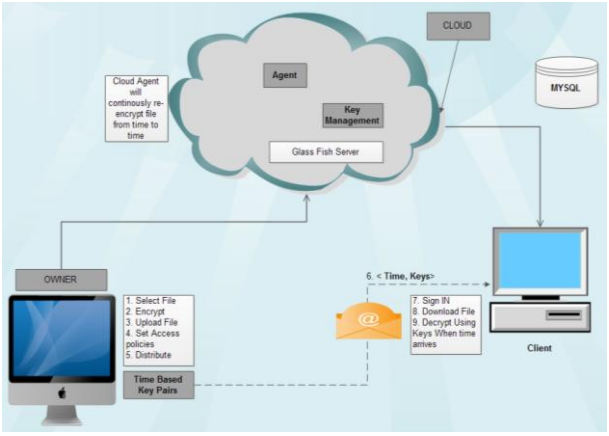

Fig:-Block Diagram

How This Works:-
step1-select the file.
step2-encrypt and upload the file.
step3-generate and distribute decryption key.
step4-sign in and download the document.
step5-decrypt the document in order to view the content of document.
step6-logout and close

III. ALGORITHM

Working of RSA Algorithm:
Step 1: Start
Step 2: Choose two prime numbers
p = 3 and q = 11
Step 3: Compute the value for 'n'
n = RSA.n_value (RSA_P, RSA_Q);
n = p * q = 3 * 11 = 33
Step 4: Compute the value for? (n)
? (n) = (p - 1) * (q -1) = 2 * 10 = 20
Int phi = RSA.cal_phi (RSA_P, RSA_Q);
Step 5: Choose e such that 1 < e <? (n) and e and n are 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)
Step 7: Stop.
Let M, is plain text (message), M= 2.
Encryption of M is: C = Me % n.
c = "" + RSA. BigMod (ar[i], RSA_E, n);
Cipher text is, C = 27 % 33.
C = 29.
Decryption of C is: M = Cd % n.
dc=dc+(char)RSA.
BigMod(Integer.parseInt(c) , d, n);
Plain text (message), M= 293 % 33.
M= 2

IV. CONCLUSION

- In this project there is advantage for adding multiple access levels for the document in order to make it more secure.
- In this project 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 privacyBy authentication and secret sharing," 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] J.H. Yeh, "A PASS scheme in cloud computing - protecting data privacy by authentication and secret sharing," Proc.

of International Conference on Security and Management, 2011.

[4] 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.

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

[6] 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.

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

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

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