Security and Data Compression in Cloud Computing Using BlobSeer Technique

Ashwin Dhivakar M R
Research Scholar, Jaipur National University, India
ashdhiv@gmail.com
Prof. D Ravichandran
Author, TATA Mc-Graw Hill, Publishing
drcplus2000@yahoo.co.in
Dr. Vijay Dakha
HOD, Computer Science & Engg , Jaipur National University
vijaypal.dhaka@gmail.com

----------ABSTRACT----------

Cloud computing environments have come up with a serious problem known as security which is in terms of Confidentiality of Data, Integrity of the Message and Authenticity of the users (CIA). Since user's personal data is being stored in an unencrypted format on a remote machine operated by third party vendors who provide various services, the impact of user's identity and unauthorized access or disclosure of files are very high. Though we have various techniques and algorithms to protect our data from hackers and intruders still cloud environments are prone to other attacks. In this paper, a novel approach is implemented to protect user's confidential data from third party service providers, and also to make sure that the data is not disclosed to any unauthentic user or the service provider even, in any cloud environments. Moreover shifting paradigm is the next major issues faced by IT infrastructures now a days. Since a huge amount of data has to get transmitted to cloud server, the "pay as you go" option hinders the consumers. This approach provides a security in terms of user authentication for "authorization" to enter the network which is made via Image Sequencing password to prove that the identity is original user, RSA algorithm to encrypt the data to provide "data integrity" and Blob-Seer, a highly parallel distributed data management service that enables to read/write and append huge data sets that are fragmented and distributed at a large scale. Thus this approach provides an overall security to the client's personal data and the issue of concurrency, volume of data can be resolved with these techniques.

Keywords - Image Sequencing, BlobSeer, RSA Algorithm, Cloud Computing, Security.

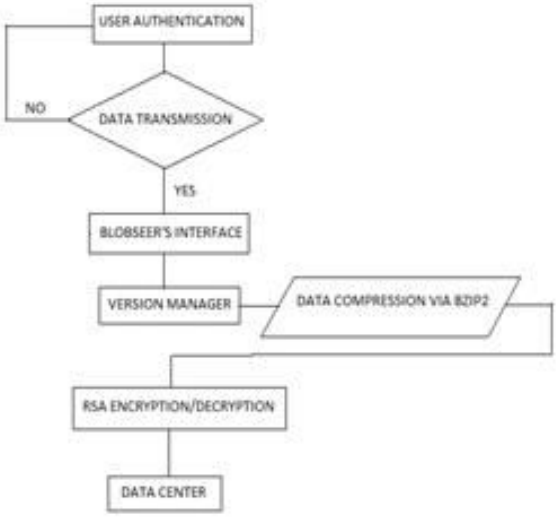
I. INTRODUCTION

Cloud Computing is one of the most impressive service offered via internet which creates a platform to store and retrieve data in a convenient way without the need of costliest hardware and it is also maintained by a third party vendor [2]. One of the most advanced features of Cloud Computing is -Virtualization which is the most effective way of delivering the user's data in a minimal amount of time and space. Cloud system provides shared resources like hardware and networks, few interfaces and services. Using cloud, it is possible to enhance the performances of applications and all services can be done only on-demand so that the computing performance is effectively maximized with irrespective of location or platform.

Cloud basically involves in data processing like storage, delivery and retrieval from a third party service providers. Cloud is totally a service oriented environment which provides three types of services namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). In Cloud Computing environment, Data and Information are very prone to attacks since resources are mostly shared among multiple servers which also allow intruders to access unauthorized data or misuse and interrupt in any form [6]. In a cloud system, user doesn't know where the data is being stored and there is no possibility for the user to take control of data where it can be allocated or scheduled only by the vendors. In order to avoid unsecured way of data processing, a multi-level approach is implemented in this paper to resolve the basic issues in cloud environments.

The prime concern on cloud computing is security and privacy of personal data or files. Cloud system allows a client to log in from any location geographically to access data, files and applications. Hence, there is a possibility of an intruder to make a security breach in any manner. So there arises a problem of Confidentiality, Integrity and Authenticity (CIA) of the data. To overcome this security issue, a novel and effective method of user authentication technique is proposed and implemented in this paper with RSA data encryption integrated with an Image Sequencing Password.

II. WORK FLOW ANALYSIS



III. RSA SECURITY ALGORITHM IN CLOUD COMPUTING

One of the commonly used Public Key algorithms is RSA which is an asymmetric key encryption or decryption algorithm [1]. Since it uses a public key to encrypt the data, which is also shared throughout but the data can only be decrypted if the private key is known to the end user.

RSA algorithm works on the cloud provider so that data is stored safe without any form of disclosure. It is also a method of security in authentication and data protection. In this algorithm, the data is stored in blocks which is called as a cipher and that is compared with a set of integers to form an encrypted data.

In this paper the RSA algorithm is integrated with Image sequencing password such that it provides a better security than any other algorithms. The data is encrypted by the service provider where as decryption is on the client side using private key which adds a multiple security layered approach so that data is securely protected.

The RSA algorithm works on the basis of three steps: key generation, encryption and decryption.

A. Key Generation

RSA involves a public key and a private key. The public key is outsourced to everyone hence it is used for encrypting the message. The encrypted message can be decrypted only using the private key with a time limit.

Key Generation Algorithm

1. Choose two distinct prime numbers x and y.
- X and Y should have the same bit length characters.
- Compute z = xy.

2. Z is the modulus function for the public and private keys. Length of z is the key length.
- Compute $\varphi(z) = \varphi(x)\varphi(y) = (x-1)(y-1) = z - (x + y - 1)$, where φ is Euler's quotient function.
- Choose an integer e such that $1 < e < \varphi(z)$ and $\gcd(e, \varphi(z)) = 1$

3. e is the public key exponent.

4. e has a short bit-length and usually $2^{16} + 1 = 65,537$.
- Determine u as $u \equiv e^{-1} \pmod{\varphi(z)}$
- i.e., $u.e \equiv 1 \pmod{\varphi(z)}$
- This is computed by using the extended Euclidean algorithm.
- u is the private key exponent.

The public key consists of the modulus z and exponent e. The private key consists of the modulus z and the exponent u, which must be kept secret. The values x, y, and $\varphi(z)$ must also be kept secret because they are used to calculate u.

B. Encryption

Public key (z, e) is used to encrypt the message M using the private key u which is kept secret. Message M is turned into to cipher text C using this expression

- C= M^e (mod z)

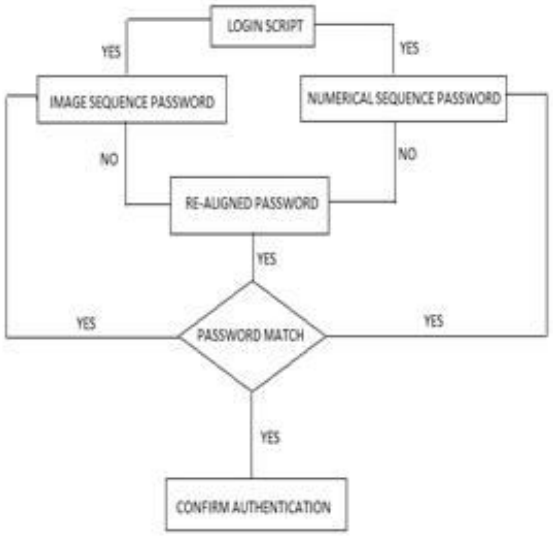
C. Decryption

Message m can be decrypted from C using the private key exponent u

- M=C^u (mod z)

IV. IMAGE SEQUENCING ALGORITHM

The Image Sequencing password is implemented where in a password sequence has to be fixed and through this way, the authentication is secured rigidly that the password always remains undisclosed except to the cloud user [3]-[5].



The Image Sequencing password is implemented wherein a password sequence has to be fixed and through this way,

the authentication is secured rigidly that the password always remains undisclosed except to the cloud user.

An algorithm is integrated with the Sequencing password so that the Images are shuffled consecutively each and every time the user log's into the system making it still more secured in terms of authenticity. Unless the sequence is known, nobody could break this system.

The next level of protection is that the sequence is not the password alone as it is seen by anyone; the position of the image sequence is the main password to log in to the cloud network. This position is interchanged always making the password secured further more. An authentic and authorized user gets into the cloud environment finally after all the authentication type which allows the user to operate securely in this system. User is not limited to passwords alone since intruders are not limited too. Therefore, data security is done through RSA algorithm which adds a multi-layered security in Cloud Computing.

V. CONCLUSION

In this paper, an analysis of the proposed security hierarchy model was examined and the result can be achieved better than the current protection techniques. The issue of Concurrency, High volume of data transmission, Integrity and Authenticity is sorted out using this security algorithm which protects data from unauthorized user and effectively maintain the resources and storage. Now the cloud service providers can adopt such techniques to attract more users and provide them any type of services in a secured environment and client's can adopt with the less utilization of resources and the storage cost is abruptly decreased.

REFERENCES

[1] Stallings, William, ―Public Key Encryption and RSA,‖ in Cryptography and Network Security, 5th ed. Published by Pearson Education, Inc, Copyright © 2011, pp. 293-314.

[2] Nicolae, B. Moise, D., Antoniu, G., Bouge, L., Dorier, M.: BlobSeer: Bringing high throughput under heavy concurrency to Hadoop Map/ Reduce applications. In: Proc.24th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2010).

[3] AlZain, Soh, Pardede, - Using Multi-clouds to Ensure Security in Cloud Computing, - in Proc. Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference, Sydney, 12-14 Dec. 2011, pp. 784 - 791.

[4] Seward, J.: Bzip2. http://bzip.org(2011).

[5] Ziv, Lempel.: A universal algorithm for sequential data compression,‖ IEEE Transations on Information Theory. Pp.337-343.

[6] Wang, Niu Liang, -Dynamic Cloud resources reservation via cloud brokerage,‖ in Proceedings of 33rd IEEE International Conference on Distributed Computing Systems (ICDCS '13), pp.400-409