2nd International Conference on Current Research Trends in Engineering and Technology
© 2018 IJSRSET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Cloud Storage Using Symmetric Alogrithm

Goswami Tushar, Solanki Jaimin, Jagveer Thakur, Mr.Trilok Suthar, Mrs. Kalyani Adwakar
Information Tehnology, Sigma Institute of Engineering, Bakrol, Gujarat, India

ABSTRACT

Now a day's users have huge amount of data that they cannot store on personal device because of limited storage hence they are move to the public clouds. As you know that cloud server is not a trusted server, so data users wants their data to be safe at cloud side. To preserve the privacy and confidentiality of documents, it should get encrypted before outsourcing to the cloud. For ensuring privacy of documents, numerous algorithms have been developed which makes user data private and avoid unauthorized access to their confidential data. Most essential characteristics of any Encryption algorithm are: Speed of Encryption and Security.

Keywords: Privacy Preserving Storage, Symmetric, Asymmetric

I. INTRODUCTION

In today's busy life, everything is digital from banking to smart studies and so Internet is the main way of communication for everyone. In Cloud, information is permanently stored at server side and then whenever client requests it received temporarily on clients hardware device which include PC's, tablets and mobile phones. Users place their data in the cloud server. Due to the increasing storage users are move to outsource more and more data to cloud server, so encryption is now the important of the hour. Encryption is the art of secret writing. Encryption transmits any information safely over the insecure transmission medium like Internet by

encoding plain text into cipher text. For encoding plain text various encryption algorithms has been proposed. The encryption algorithms are categorized into two types: first is Symmetric key encryption and second is Asymmetric key encryption.

In Symmetric key encryption same key is used to encrypt and decrypt the data. The key has to be shared before transmission to sender and receiver. 3DES, RC5, Blowfish, Twofish, Cast, AES are examples of symmetric Key encryption algorithms.

In Asymmetric key encryption, there is key-pair; private key and public key. Public key is used for encryption of data and private key is used for decryption of the encrypted data.

II. RELTED WORK

An algorithm is basically a formula for solving a data snooping problem. An encryption algorithm is a set of mathematical procedure for performing encryption on data. Through the use of such an algorithm, information is made in the cipher text and requires the use of a key to transforming the data into its original form. This brings us to the concept of

cryptography that has long been used in information security in communication system.

III. PROPOSED SYSTEM

Fig.1 Architecture of proposed system

IV. OVERVIEW OF TWO ALGORITHMS

A. Symmetric

Symmetric algorithm is the simplest kind of encryption that has only one secret key to cipher and decipher information. Symmetric encryption is old and one of the well know technique. It uses a secret key that can either a number, a string of random numbers or may be a word. It is merged with a plaintext message to change in some randomly message that cannot be understand by any third party. The main disadvantage is that the secret symmetric key should be share between sender and receiver before the decrypt.

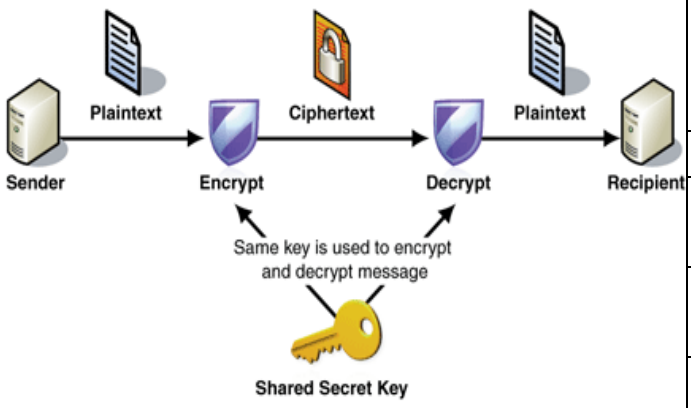


Fig.1 Symmetric Encryption Scheme

B. Asymmetric

Asymmetric algorithm proposed a new type of cryptography that distinguished between encryption and decryption keys. One of the key would be publicly known and the other would be kept private by its owner.

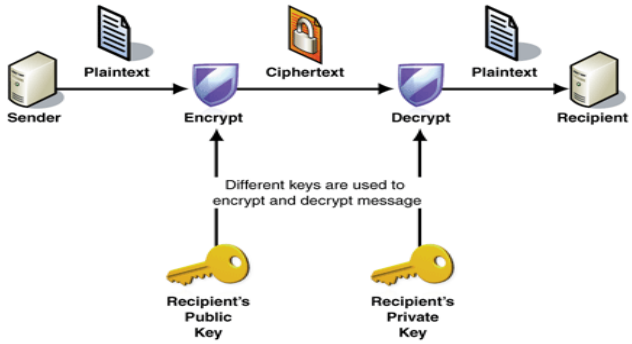


Fig. 2 Asymmetric Encryption Scheme

1) Each user generates a pair of keys to be used for the encryption and decryption of message.
2) Each user places one of the two keys in a public register. This is the public key. The companion key is kept private.
3) If bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4) Alice decrypts the message using her private key.

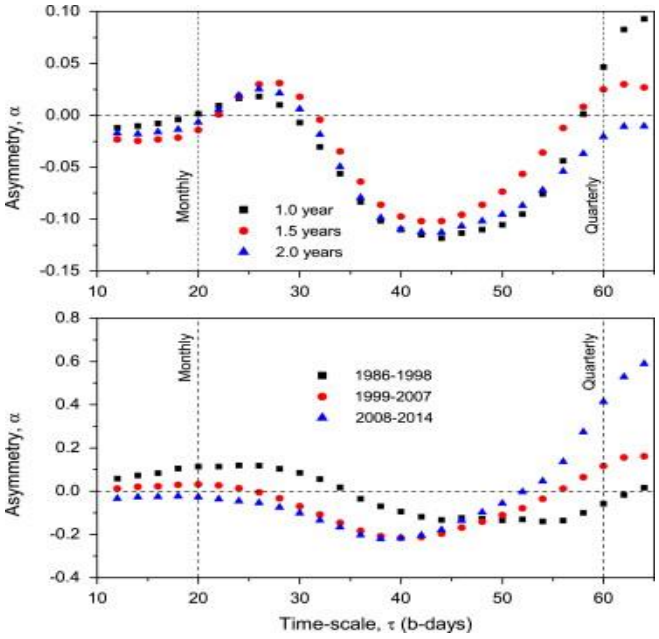
Table .1 Comparison Chart

Symmetric	Asymmetic
Same key is used for encryption and decryption	One key for encryption and other key for decryption
Very fast	slower
Key exchange is big problem	Key exchange is not a problem
Also called secret key encryption	Also called public key encryption
The key must be kept secret	One of the two keys must be kept secret
The sender and receiver must share the algorithm and the key	The sender and receiver must have one of the matched pair of keys.

V. EXPERIMENTAL DESIGN

For experiment purpose, we have used one pc with IntelI CoreI i3-4005U CPU@ 1.70 GHZ CPU with 4GB RAM.

We implemented the algorithms according to their standard specifications in Java Runtime environment using Java, on Windows 7 Operating System. In the experiment we encrypt the pdf, text, Doc files of different size ranges between 15KB to 400KB and calculate their mean encryption time.



Above graph illustrates time comparisons between Twofish and Blowfish. Twofish takes less time to encrypt the document than Blowfish.

VI. CONCLUSION

When it comes to encryption, the latest schemes may necessarily the best fit. You should always use the encryption algorithm that is right for the task at hand. In fact, as cryptography takes a new shift, new algorithm are being developed in a bid to catch up with the eavesdroppers and secure information to enhance confidentiality. Hackers are bound to make it tough for experts in the coming years, thus expect more from the cryptographic community.

REFERENCES

[1]. Schneier, J. Kelsey, D. Whiting, D. Wagner,C. Hall, and N. Ferguson, "TwoFish: A 128-bit Block Cipher", AES submission, june 1998.

[2]. Nikhil Joshi, Jayachandran Sundarajan et.al. "Tamper Proofing by Design using generalized involution-based concurrent error detection for involutional Substitution Permutation and Feistel Network" IEEE Transaction on Computer, October 2006

[3]. Dr. S.A.M Rizvi, Dr. Syed Zeeshan Hussain et.al "Performance Analysis of AES and TwoFish Encryption Schemes", International Conference on Communication Systems and Network Technologies 2011

[4]. Shun-Lung Su, Lih-Chyau Wuu, and Jhih-Wei Jhang, "A New 256-bits Block Cipher – Twofish256"

[5]. Shiho Moriai, Yiqun Lisa Yin. "Cryptanalysis of Twofish (II)".Technical Report, IEICE, ISEC2000-38, 2000.