International Journal of scientific research and management (IJSRM)
||Volume||4||Issue||11||Pages||4744-4746||2016||
Website: www.ijsrm.in ISSN (e): 2321-3418

Superiority of Twofish over Blowfish

Deepali D. Rane
Assistant Professor
Department of Information Technology,
D.Y. Patil College of Engineering, Akurdi.
deepalirane35@gmail.com

Abstract- Now a day's users are generating huge amount of data and hence they are motivated to outsource it to the public cloud. As cloud server is not trusted server, so data users wants their data to be safe at cloud side. To preserve the privacy of documents, it should get encrypted before outsourcing to the cloud. For ensuring privacy of documents, numerous algorithms have been proposed 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. In this Paper, speed comparisons between two algorithms i.e. Twofish and Blowfish have been studied. We have analyzed encryption speed of both algorithms by encrypting different sized data. Performance has been calculated in terms of throughput of each algorithm on different sets of data.

Keywords: Privacy Preserving Storage, Cloud Twofish, Blowfish

I. INTRODUCTION

In today's vast life, everything is digital from banking to Emails 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 cached temporarily on clients space which include PC's, tablets and mobile phones. It is an Internet based computing which enables sharing of various services. Users place their data in the cloud server. However, the fact is that users no longer have physical possession of their possibly large size of outsourced data. Due to the increasing storage and computing requirements users are motivated to outsource more and more data to remote server, so encryption is now the necessity of the hour. Encryption is the art of secret writing. Encryption stores and 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, 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. Length of Key plays as important role in Symmetric key encryption. 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. In secure

communication , Symmetric Encryption Schemes perform the real part of encrypting data as they are very fast and Asymmetric Encryption Schemes take the responsibility of distributing keys.DES (Data Encryption Standard) was the most popular encryption algorithm but it was surrounded by controversy as many cryptographers objected to the "closed-door" design of the algorithm. When DES gets cracked there was need for highly secure encryption standard. In 1997, in response to the desire to replace DES algorithm with stronger and more reliable algorithm, NIST announced public request for an encryption standard, called Advanced Encryption Standard (AES). Twofish and Rijndael were the two algorithms out of 5, selected as finalists of the competition in second round; **Twofish** is designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner and **Rijndael** by J. Daemen & V. Rijmen. Rijndael was the winner of competition and became the Advanced Encryption Standard (AES).

DOI: 10.18535/ijsrm/v4i11.01

II. RELTED WORK

Bruce Schneier in [1] has described different aspects of Twofish algorithm for encryption of different type and size documents. He has demonstrated working of Twofish along with components of its system architecture which includes MDS matrices, PHT, S-Boxes and complex key schedule. A research of [2] has proposed a system in which authors have focused on tamper proofing techniques that use low cost involution based time redundancy concurrent error detection schemes involving SPN and FN. Twofish (AES Finalist) show that low cost for detecting all transient faults can detect all single bit permanent faults & >99% of all multiple bit permanent faults.

Dr. S.A.M Rizvi in [3] analyzed two popular encryption algorithms: AES and Twofish. From the simulation result they have found that AES is faster than Twofish, but with increasing Ram Twofish becomes faster than AES. For sound and image encryption Twofish has better performance than AES. Shun-Lung Su [4] has proposed a modified version of Twofish in which instead of 128 bit input block, they have expanded input to 256 bit block size. This new cipher has 10 rounds of Feistel network instead of traditional 16 rounds of Feistel network.

III. PROPOSED SYSTEM

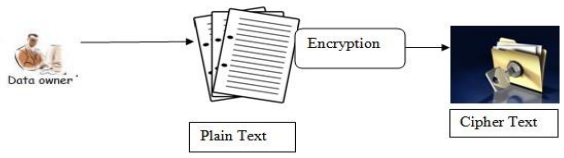


Fig.1 Architecture of proposed system

IV. OVERVIEW OF TWO ALGORITHMS

A. *TwoFish*

Twofish is a 128-bit symmetric block cipher and it accepts variable-length key ranging up to 256 bits. Twofish is based on a Feistel network and it has 16 rounds. Bijective function F is made up of four key-dependent 8 by 8 bit S-boxes followed by a fixed maximum distance separable matrix. Pseudo-Hadamard transform is a simple 32bit mixing operation. Twofish has very complex key schedule.

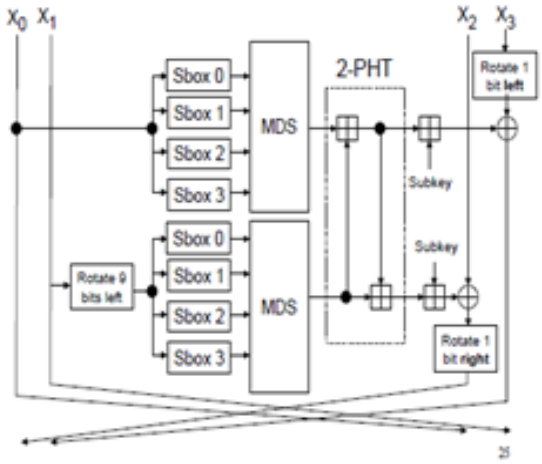


Fig.1 Twofish Encryption Scheme

Twofish was developed and designed to meet NIST's design criteria for Advance Encryption Standard (AES) which includes key lengths of 128 bits, 192 bits, and 256 bits. It is a 128-bit symmetric block cipher. It is Efficient on both Intel Pentium Pro and other software and hardware platforms. There are no weak keys and it has Flexible design.

B. *BlowFish*

In 1983, Bruice Schneier developed algorithm as alternative to aging DES and IDEA namely Blowfish. It is symmetric key block cipher. Blowfish has 64-bit block size and variable key length from 32bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. Blowfish is known to be susceptible to attacks on reflectively weak keys. Blowfish is in public domain that is it is license free and opens for everyone. Blowfish splits 64 bit input into two halves each of 32 bit and then according to Feistel structure cipher text will get produced from plain text.

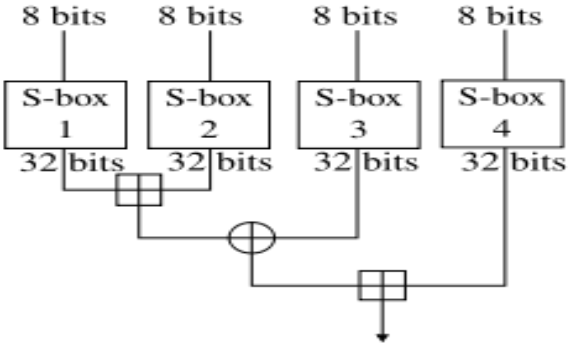


Fig. 2 Blowfish Encryption Scheme

Table .1 Comparison Chart

Blowfish	Twofish
Alternative to the aging DES	Modified version of Blowfish
block size of 64 bits	block size of 128 bits
keys- 32 – 448 bits	128,192,256 bit keys
----------	Finalist of NIST to become the AES standard
Blowfish is known to be susceptible to attacks on reflectively weak keys	No weak Keys
Less Cryptanalysed	Extensively Cryptanalysed
Safety Factor<2	Safety Factor=2.67
Uses Key dependant s-boxes	Uses Pre computed key dependant S-boxes and complex key schedule

V. EXPERIMENTAL DESIGN

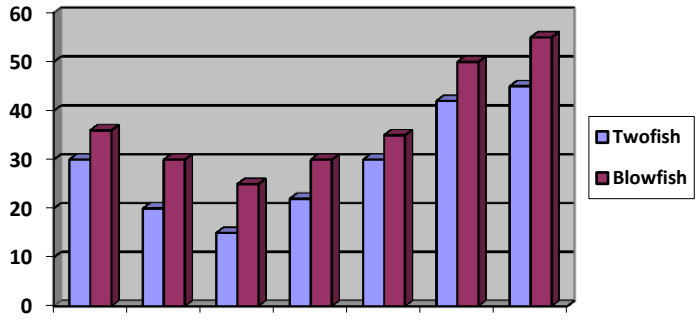
For experiment purpose, we have used one pc with IntelI CoreI i3-4005U CPU@ 1.70 GHZ CPU with 4GB RAM.

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.

Table.2 Time Comparison between Twofish & Blowfish

File size (in Kb)	TwoFish	Blowfish
15	30	36
35	20	30
93	15	28
157	22	32
211	30	39
293	42	50
400	45	60

According to the results found, as the data size increases the time to encrypt the data also increases. If the time to encrypt the data by Twofish and Blowfish get compared then we can find that Twofish encrypts data in lesser time.



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

VI. CONCLUSION

In this paper, we have analyzed two popular encryption algorithms: TwoFish and BlowFish.

We discussed the basic design and performance issues of two algorithms. It has been found that both the algorithm have Feistel network and both are open source algorithms.

From the experimental results, we found that for text encryption, TwoFish requires lesser time than BlowFish. Size of RAM affects more the performance of TwoFish.

In future we intend to conduct the experiments in varying hardware and software environment to evaluate the performances of these algorithms.

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.