ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 7, July 2016**

# Enhanced Security using Hybrid Encryption Algorithm

Neha, Mandeep Kaur

M.Tech. Student, Department of Computer Engineering, RBIEBT, Mohali, India

Assistant Professor, Department of Computer Engineering, RBIEBT, Mohali, India

**ABSTRACT**: Information Security plays a major role in today's scenario. Cloud computing is a technology that provides access to information and computing resources from anywhere that a network is available. There is a need to secure the data stored on cloud. The main goal behind the design of encryption algorithm must be security against unauthorized attacks. However, for all cloud computing applications, performance and cost of implementation are also major concerns. Encryption algorithm would not be of much use if it is very much secure but slow in performance. The security and performance of encryption algorithms must be balanced. In this paper, encryption algorithms (AES, Blowfish, Twofish) has been discussed to analyze the performance level of each algorithm.

**KEYWORDS**: cloud computing, security, privacy, authentication, confidentiality, AES, Blowfish, Twofish.

## I. INTRODUCTION

Cloud Computing is the delivery of computing resources over the internet everything ranging from applications to data centers. It provides the on-demand services on a pay as you use basis. Cloud is something present at remote locations such as Internet. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. Cloud computing and its solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It provides various types of services such as SaaS, PaaS and IaaS.

**The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST):**
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

### 1.1 Deployment models of cloud computing

In Cloud computing, available deployment models are:

#### 1.1.1Public Cloud:

Every user can access the public cloud from anywhere. It can be accessed using interfaces such as internet browsers. Users have to pay only for that time duration in which they user the cloud service i.e., pay-per-use model. Example of public cloud providers includes Amazon AWS, Microsoft etc.

#### 1.1.2 Private Cloud:

Private cloud exists within an organization's internal enterprise data centre. Only that user can access the private cloud that is having authorized access by the organization. Security can be easily managed using private cloud. Example of private cloud is intranet.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

**1.1.3 Hybrid Cloud:**
It provides the functionalities of both public and private cloud. Data and applications can be secured in an efficient manner. In hybrid cloud, one can take advantage of third party cloud providers in either a full or partial manner, thus increasing the flexibility of cloud computing.

**1.1.4 Community Cloud:**
A community cloud is a multitenant cloud service model that is shared among various organizations. It is managed and secured by every organization participating. It is hybrid form of private clouds designed specifically for a targeted group.

**1.2 Deployment models of cloud computing**

In Cloud computing, there are three service models:

**1.2.1 Software as a Service (SaaS)**
It provides software's as a service to the users according to their requirements. It allows the users to use the services that are hosted on the cloud server.
Examples include: Email, ERP, CRM etc.

**1.2.2 Platform as a Service (PaaS)**
Clients are provided platform access, they can run their own applications and customized software's on the clouds without having to worry about maintaining hard drives and servers.
Examples include: Google App Engine, Microsoft Azure etc.

**1.2.3 Infrastructure as a Service (IaaS)**
It is a way of delivering cloud computing infrastructure such as servers, storage, network capacity, and other basic computing resources as an on-demand service. It enables the organizations to run entire data centre application on clouds without the need of any infrastructure.
Examples include: Flexiscale, AWS: EC2 etc.

## II. RELATED WORK

In [9] authors have studied twofish algorithm and modifies it by keeping delay as the main constraint. They have modified the MDS matrix and PHT in twofish algorithm. This in turn modifies the F function of twofish algorithm. They compared twofish of 128-bit key with the modified twofish of 128-bit key and concluded that modified twofish has less delay than twofish. They have also compared twofish of 192-bit key with modified twofish of 192-bit key and analyzed that modified algorithm has less delay than the conventional one.
In [11] authors discussed the various problems associated with cloud computing like data privacy, security, accessibility and reliability etc. But the most important between them is security and how cloud provider assures it. In this paper, the proposed work plan is to remove the issues regarding data privacy using encryption algorithms to enhance the security on cloud. He proposed various encryption algorithms such as AES, DES, RSA and Blowfish that will enhance the performance of cloud. He proposed the model through which we can compare these algorithms and can determine the best algorithm in terms of providing security to the cloud.
In [14] authors analyzed and found an efficient encryption algorithm which takes less space among these encryption algorithms such as DES, TDES, AES, Blowfish and Twofish. After analyzing above result we found that TDES is better than all these algorithms. DES takes less space than TDES but DES is not a secure algorithm because after 2^56 imagination brute force attack can crack this algorithm. TDES is strong algorithm but it also takes almost two times more space than DES.
In [15] authors proposed a hybrid model which uses a combination of two symmetric algorithms enhanced AES and Blowfish for data confidentiality, Message Digest-5 for data integrity, Elliptic Curve Diffie Hellman algorithm-ECDHA for key exchange and Elliptic Curve Digital signature algorithm-ECDSA is used for digital signature. In this, AES is enhanced by modifying the S-boxes columns, and then the combination of enhanced AES and blowfish is used for data confidentiality. Performance of this system is evaluated on the basis of encryption/decryption time, throughput and memory usage for different data formats like text file, image file, audio file and video file.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

In [16] authors surveyed the various techniques of cryptography and compare them to determine the best technique for security. They have described particularly four algorithms i.e. AES, DES, TDES and Blowfish and compare them according to their encryption times. They concluded that Blowfish is better in terms of speed followed by AES. Other algorithm such as 3DES has least efficient performance as compared to other. In future, Encryption techniques can be used in such a way that it can consume less time and power.

## III. PROPOSED SYSTEM

To secure the cloud, various encryption/decryption algorithms are used to store the data on cloud in encrypted form and retrieve the data from cloud in decrypted form.

### 2.1 Algorithms used

**AES**

AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.
AES performs following steps for encryption/decryption:

- First step is to generate round keys, round keys are generated using Rijndael's key schedule.
- The plaintext is converted to 4 x 4 state matrix.
- Each byte of the state is combined with the round key using bitwise xor.
- This is followed by ten rounds. In each of the first nine rounds, it performs four steps.
- Byte substitution in which each byte of state is replaced with the byte of S-Box in case of encryption and with the byte of Inverse S-Box in case of decryption depending upon its value.
- Shift rows in which first row of state matrix remains unchanged, second row shifts by 1 bit to the left, third row shifts by 2 bits to the left and fourth row shifts by 3 bits to the left. In case of decryption, shifting is to the right.
- Mix Columns in which each byte is replaced by a value dependent on all 4 bytes in the column.
- Fourth step is Add Round Key in which each byte of the state is combined with the round key using bitwise xor.
- In last round, it performs three steps only, the mixcolumns step is not performed in last step.

**BLOWFISH**

Blowfish is a symmetric block cipher designed by Bruce Schneier in 1993. It is a variable length key, 64-bit block cipher. It uses a 32 to 448 bit key.
It consists of two parts:

The expansion of the key: break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.
The encryption of the data: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).

- The input is a 64-bit data element, x.
- Divide x into two 32-bit halves: xL, xR.
- Then, for i = 1 to 16.
- xL = xL XOR Pi xR = F(xL) XOR xR
- Swap xL and xR
- After the sixteenth round, swap xL and xR again to undo the last swap.
- Then, xR = xR XOR P17 and xL = xL XOR P18.
- Finally, recombine xL and xR to get the cipher text

**TWOFISH**

Twofish is a 128-bit block cipher that accepts a variable-length key up to 256 bits. The cipher is a 16-round Feistel network with a bijective F function made up of four key-dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

distance separable matrix over GF($2^8$), a pseudo-Hadamard transform, bitwise rotations, and a carefully designed key schedule.

- The plaintext is split into four 32-bit words.
- In the input whitening step, these are xored with four key words.
- This is followed by sixteen rounds. In each round, the two words on the left are used as input to the *g* functions. (One of them is rotated by 8 bits first.)
- The *g* function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on an MDS matrix.
- Each S-box takes 8 bits of input, and produces 8 bits of output.
- The four results are interpreted as a vector of length 4 and multiplied by the 4X4 MDS (maximum distance separable) matrix.
- The results of the two *g* functions are combined using a Pseudo- Hadamard Transform (PHT), and two keywords are added.
- These two results are then xored into the words on the right (one of which is rotated left by 1 bit first, the other is rotated right afterwards).
- The left and right halves are then swapped for the next round.
- After all the rounds, the swap of the last round is reversed, and the four words are xored with four more key words to produce the ciphertext.

**2.2 Methodology**

The architecture that can be followed to determine the performance of hybrid encryption algorithm is as follows:

- Sender's System Architecure

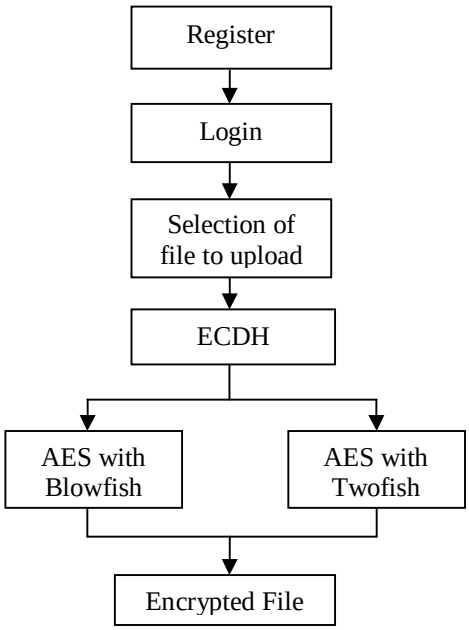


Figure1. Sender's system architecture

1. Register and Login with correct login information.
2. Select a file which you want to upload.
3. Apply ECDH for key generation.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

4. Apply AES with Twofish or AES with Blowfish on selected file that will generate encrypted file.

**Receiver's System Architecture**

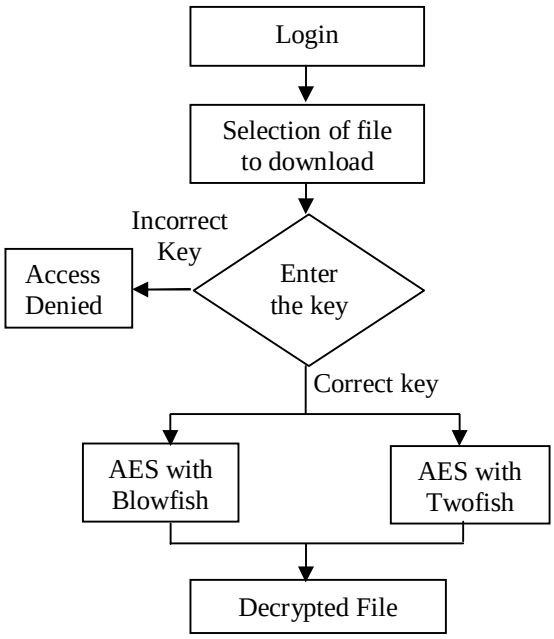


Figure2. Receiver's System Architecture

1. Login with correct login information.
2. Select a file which you want to download from the cloud.
3. Enter the correct key to download file.

   -If key is correct then allow access to download otherwise access denied.
4. If key is correct then Apply AES with Twofish or AES with Blowfish to decrypt the file.
5. Hence, the file will be downloaded.

The hybrid of AES and Twofish can provide more security as well as high performance. ECDH (Elliptic curve Diffie Hellman) mechanism can be used for key generation. This methodology is used to evaluate performance of hybrid AES+Blowfish and Hybrid AES+Twofish.

## IV. RESULTS

Text files have been chosen for encryption and decryption of cloud data. This methodology can be implemented using Eclipse and java programming language. Both the hybrid algorithms can be compared on the basis of:

1. Encryption Time.
2. Decryption Time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Two different files of 76 kb and 103 kb have been taken and their encryption/decryption time has been calculated using the above methodology. Following are the graphs showing the comparison of encryption and decryption time. Figure3 and Figure4 both shows hybrid of AES and Twofish provide better results as compared to hybrid of AES and Blowfish in terms of encryption/decryption time.

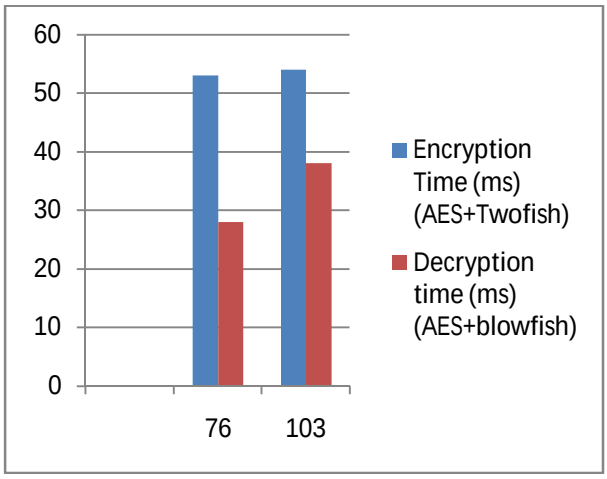


Figure3. Comparison of Encryption Time

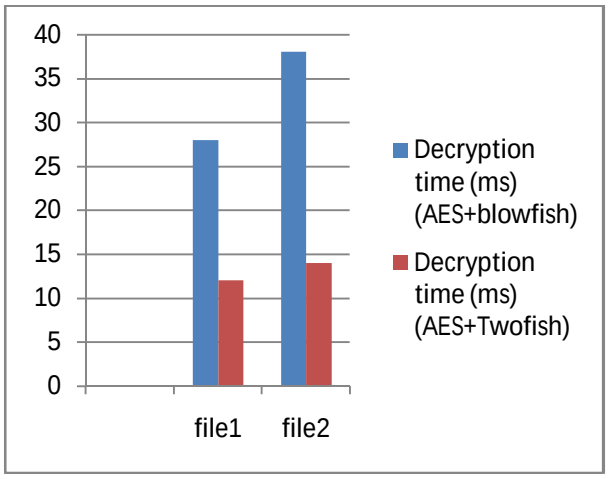


Figure4. Comparison of Decryption Time

## V. CONCLUSION AND FUTURE SCOPE

Security is the major factor of cloud computing. To achieve security, various cryptographic algorithms are used to encrypt and decrypt the data. But the cryptography algorithm with high security and low performance is not acceptable. In this paper, we discussed three techniques AES, Blowfish and Twofish. As analyzed, Twofish will give better performance than blowfish. Because as compared to Blowfish, Twofish is a 128-bit block cipher and uses at most 128-bit key. Twofish is much faster, its key setup is as fast as 1.5 encryptions where as Blowfish is slow in setting up a key, taking as long as 521 encryptions. Blowfish is not suitable for smartcards since it requires more memory where Twofish is efficient for smartcards. In case of Twofish, S-Boxes are constructed carefully to make sure that all S-Boxes are strong. Twofish has no weak keys whereas Blowfish has weak keys. This paper shows comparison on the basis of encryption/decryption time and hybrid of AES and Twofish takes less time to encrypt and decrypt the file as compared to AES and Blowfish.

This work can be extended to determine the performance of cloud in terms of throughput, power consumption and memory consumption. This work can also be extended to the use of large size of text files, images, audio files and video files for encryption and decryption.

## REFERENCES

[1] Tingyuan Nie and Teng Zhang , "A study of DES and Blowfish encryption algorithm", IEEE Region 10 Conference, 2010.

[2] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, Vol. 14, No. 5, pp. 14-22, 2010.

[3] S. Kamara, and K. Lauter, "Cryptographic cloud storage", Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 136-149, 2010.

[4] Nidhi Singhal, and J. P. S. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization", International Journal of Computer Trends and Technology, Vol. 2, No. 6, pp. 177-181, 2011.

[5] M.Pitchaiah, Philemon Daniel, Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research, Vol. 3, Issue 3, 2012.

[6] S. Zarandioon, D.D. Yao and V. Ganapathy, "K2C: Cryptographic cloud storage with lazy revocation and anonymous access", Security and Privacy in Communication Networks, Springer Berlin Heidelberg, pp. 59-76, 2012.

[7] Gurpreet Kaur and Manish Mahajan , "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms", International Journal of Engineering Research and Applications, Vol. 3, No. 5, pp. 782-786, 2013.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 7, July 2016**

[8] Sajjad Hashemi (2013), "Data storage security challenges in cloud computing", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 2, No. 4, pp. 123-133, 2013.
[9] Purnima Gehlot, S. R Biradar and B. P. Singh, "Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL", International Journal of Computer Applications, Vol. 13, pp. 37-42, 2013 .
[10] Anshu Parashar and Rachna Arora, "Secure user data in cloud computing using encryption algorithms", International journal of engineering research and applications, Vol. 3, Issue 4, pp. 1922-1926, 2013.
[11] Mandeep kaur and Manish Mahajan , "Using encryption algorithms to enhance the data security in cloud computing", International Journal of Communication and Computer Technologies, Vol. 1, No. 12, pp. 56-59,2013.
[12] Prerna Mahajan & Abhishek Sachdeva , "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol. 13, Issue 15, 2013.
[13] Nikhil Gajra, Shamsuddin S. Khan and Pradnya Rane, "Private Cloud Security: Secured Authentication By Using Enhanced Algorithm", International Conference on Advances in Communication and Computing Technologies, 2014.
[14] MD Asif Mushtaque Harsh Dhiman and Shahnawaz Hussain Shivangi Maheshwari, "Evaluation of DES, TDES, AES, Bowfish and Twofish encryption algorithm: based on space complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3, Issue 4, pp. 1922-1933, 2014.
[15] A. P Shaikh and V. kaul, "Enhanced security algorithm using hybrid encryption and ECC", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 6, Issue 3, pp. 80-85, 2014.
[16] Mitali, Vijay Kumar and Arvind Sharma , "A Survey on Various Cryptography Techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3, Issue 4, 2014.
[17] Saurin Khedia and Nishant Khatri, "A review on hybrid techniques of security in cloud computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11, pp. 243-256, 2014.
[18] Pulkit Chaudhary , "Security concerns and privacy issues in cloud computing", International Journal of Current Engineering and Technology, Vol. 4, No. 6, 2014.