*THINK INDIA JOURNAL*

ISSN:0971-1260
Vol-12- Issue-12-November-2019

# Hybrid Des-Blowfish Cloud Data Security Model

**Namarta Vij**
School of Computer Science and Engineering,
Lovely Professional University,
phagwara, punjab, india

**Manpreet Kaur**
Department of Computer science and Engineering,
Guru Nanak Dev University, Amirtsar

**Balraj Singh**
Department of Computer science and Engineering,
Guru Nanak Dev University, Amritsar

**ABSTRACT- Cloud computing is used ubiquitously not only by the local users but also by industries. In cloud computing, the security of the data on servers is an intriguing issue. This paper proposes a method for the security of cloud through key generation and encryption. In our proposed work, the keys such as OTP, Secret key, Identification key and Sharing key are generated in the email of the user upon registering. Whenever the user wants to store the file as an attachment in the cloud storage for encryption, the user has to provide the OTP. After that, the user has to provide the secret key for the encryption which is being performed by DES, CAST, BLOWFISH, DES with CAST and DES with BLOWFISH algorithms to file of any size. When the users want to insert, download and view the files in the cloud storage, they have to specify the identification key. The analysis shows that the proposed hybrid DES with BLOWFISH algorithm provides higher complexity and lesser execution time for encryption and decryption than individual algorithms.**

**Keywords:** cloud computing; cryptography; encryption; decryption; key generation; file size; symmetric encryption; des.

## 1. INTRODUCTION

Cloud computing is used tremendously all over the world as it provides easy and flexible access to applications without concerning about the platform, infrastructure, and software[10]. Though cloud computing is expedient in many ways but still it has consequences and one of the issue is the security. Enterprises still wonder if they should take the risk of migrating their confidential data to the cloud. Many of the companies are using it but security remains a serious concern. The RSA conference cloud security alliance [12] held on 4th march listed the "Treacherous 12", the 12 security threats related to cloud computing the enterprises face in 2016 which includes:

i. Data Breaches
ii. Broken authentication
iii. Hacked API's and interfaces
iv. Account hijacking
v. The APT parasite
vi. Permanent data loss
vii. Inadequate diligence
viii. Cloud server abuses
ix. DOS Attacks
x. Malicious intruder
xi. Shared technology, shared danger
xii. Exploited system vulnerabilities

ISSN:0971-1260
Vol-22- Issue-35-December-2019

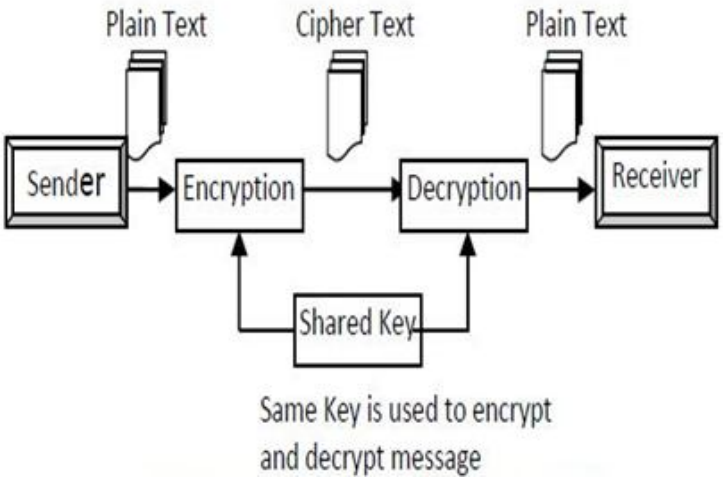


**Figure 1** Symmetric Encryption and Decryption

The technique of Cryptograph is used to provide security in cloud computing models[2]. The security can be provided by the use of symmetric as well as asymmetric algorithms of the cryptography.

The algorithms are briefly discussed below:

*1.1 DES*

DES (Data Encryption Standard) is a symmetric block cipher algorithm developed by IBM in 1975. It has a key size of 56 bits and block length of 64 bits with 16 rounds and fast computational speed. The algorithmic structure of this algorithm is balanced Feistel network with low power consumption and high memory usage. It provides security against brute force attacks. The general structure of DES is shown below:

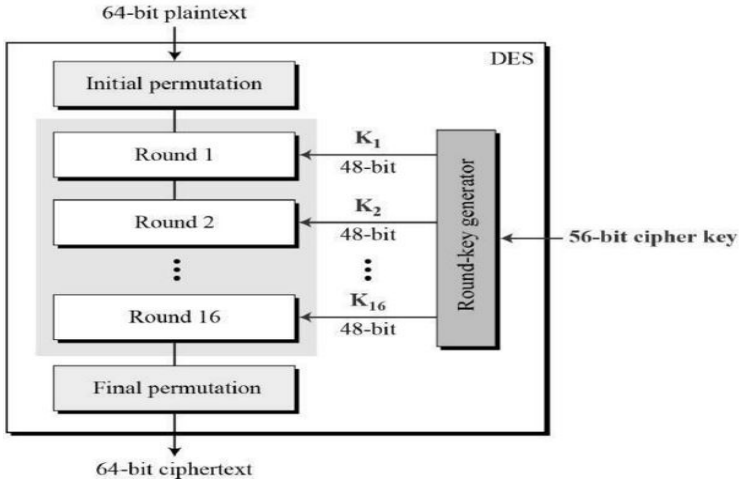


**Figure 2** General structure of DES

*1.2 CAST*

CAST is a symmetric block cipher algorithm developed by Carlisle Adams and Stafford Tavares in 1996. It has a key size of 40 to 128 bits and block length of 64 bits with 12 to 16 rounds. When the size of the key is greater than 80 then only full 16 rounds are used other-

ISSN:0971-1260
Vol-12- Issue-12-November-2019

wise it uses 12 rounds only. The algorithmic structure of this algorithm is balanced Feistel network.

*1.3 BLOWFISH*

BLOWFISH is a symmetric block cipher algorithm developed by Bruce Schneier in 1993. The algorithmic structure of this algorithm is balanced Feistel network with very high encryption and decryption throughput [10]. It has very high power consumption and low memory usage of less than 5kb. It provides security against dictionary attacks.

Paper includes the following sections:
In section 2 briefly explain about Literature work in the area of cloud computing and the cloud security. Section 3 emphases on problem formulation in which detailed description of the algorithms and their working is illustrated in the form of algorithms. Section 4 emphasize on the proposed work. In the section 5 experimental setup explain, which is used in order to carry out proposed work and also shows the results which are obtained. Section 6 and 7 emphasize on future work

## 2. LITERATURE WORK

The need for securing the cloud has emerged since the use of well-known technology cloud computing has emerged. Many authors are contributing to secure this widely used platform by using the encryption algorithms[11] determines the security of CAST-256 based on linear cryptanalysis and constructs a basic algorithm as shown in fig 9. The results in their paper conclude that the CAST algorithm with 64 bits key length based on 8*32 S-boxes is much secure for linear cryptanalysis. Analyse the data encryption performance of data, sound, text and images based on different key length and file size using blowfish algorithm and evaluates the security and speed of the algorithm. He proves by equating the mathematical equations that upon changing the key length no effect occurs but upon changing the file size the processing time gets affected. studies DES and BLOWFISH algorithm and evaluates the encryption speed of both of these algorithms based on varies memory sizes[16]. In addition, they also performed a runtime comparison of both of the algorithms which show that blowfish takes less time to encrypt the data. The results conclude that the Blowfish executes faster than the DES. Represent the various security issues in cloud deployment models and cloud service delivery models and challenges to the cloud computing such as security, costing models, charging models, service level agreement and cloud interoperability issues[14].
In the recent study developed the hybridization of DESCAST algorithm which can be used in data of size less than 1MB and analyses the computation time for encryption is more than CAST and DES algorithm[12]. The main efficiency drawback of this paper is that it is slow on big data.The findings are also affirmed by other author who describes various techniques for securing client's data which includes authentication interface, single encryption, and multi-level virtualization[6]. The comparison is shown between DES, CAST, RC6, Blowfish and IDEA algorithms with different key sizes and block lengths to evaluate execution time of each algorithm for key generation, encryption and decryption and throughput of encryption and decryption of each algorithm. They conclude that RC6 is faster in execution than other algorithms and Blowfish and RC6 have the same throughput[5].analyses the security of BLOWFISH algorithm using correlation and avalanche coefficient. They presented the basic architecture of Blowfish algorithm along with its F-function architecture. The results analysis shows the avalanche text for four rounds which includes first, second, third and last round from which second round proves to be best and also shows the summary for values of the correlation coefficient[18].Investigate the issues of security from different perspectives. They

 

ISSN:0971-1260
Vol-22- Issue-35-December-2019

investigate in detail the key security issues in cloud computing environment and the solutions for this environment [16]. Presents an authentication framework to provide data gathering and sharing which is operated by both user and admin and can provide security to cloud user based on RSA and MD5 algorithms of cryptography [17]. Identify security requirements and categories of threats and presents solutions for the security threats [20]. They introduce trusted a third party for maintaining the authenticity, confidentiality, and integrity of data.

## 3. MAJOR SECURITY ALGORITHMS

This section will discuss and present in detail about three different security algorithms.

### *3.1Data Encryption Standard*

DES is a method which takes 64bits as input of plaintext and provides 64 bits of ciphertext as output. It has a key length of 56 bits which means it can provide security of $2^{56}$. The rounds of DES consist of a function which operates in four steps: an expansion permutation, a whitener, a substitution-permutation, a straight permutation.

#### *3.1.1 Key Generation*

Key Generation phase creates a 48-bit key out of 56-bit cipher key as it drops 8 keys for parity check. It divides the entire 56-bit key into two groups of 28 bit each and performs a circular left shift in these two groups. After this, these two groups are compressed and 48 bits subkey is selected by 24-bit from left and 24-bit from the right.

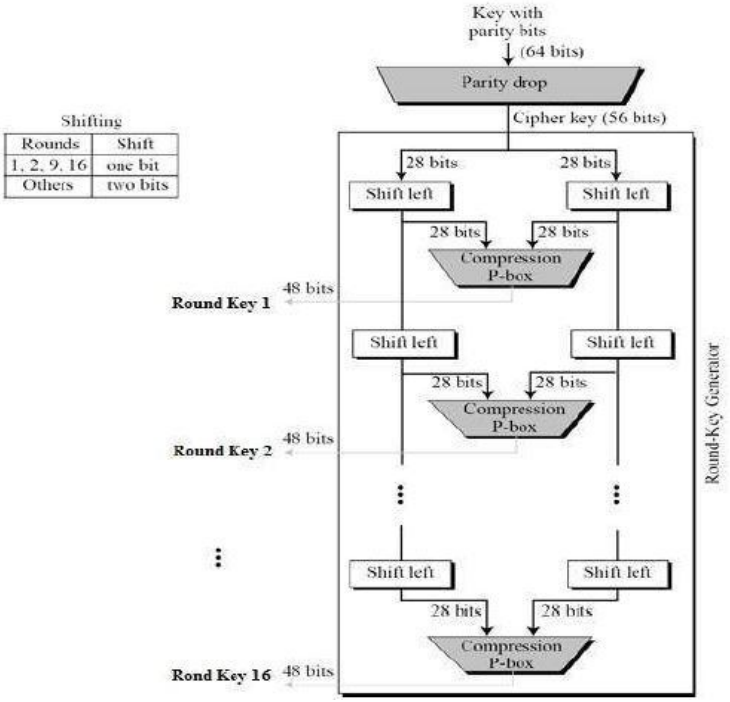


**Figure 3** DES Key Generations

#### *3.1.2 Encryption and Decryption*

ISSN:0971-1260
Vol-12- Issue-12-November-2019

It consists of round function f in which 48-bit key produced in key generation phase is applied to 32-bit right block to produce 32- bit output.

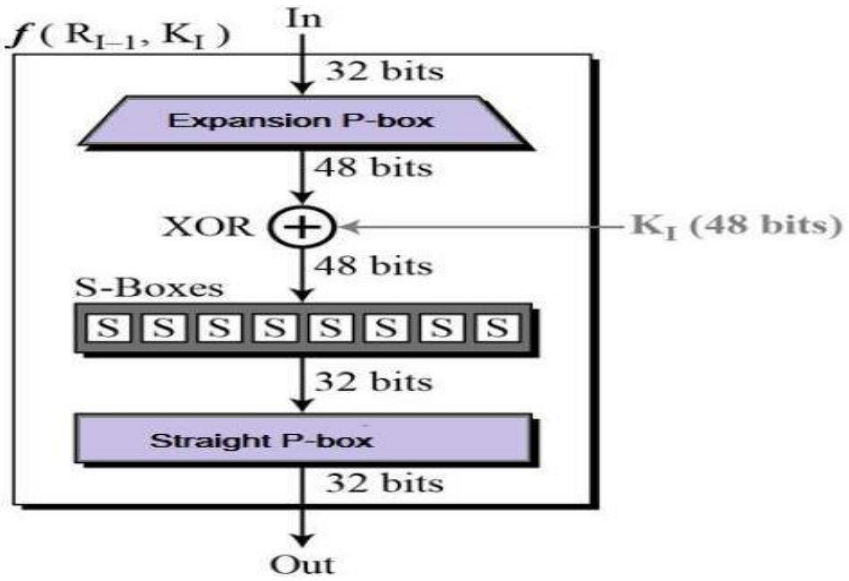


**Figure 4** DES Encryption and Decryption

The functioning of the DES encryption and decryption process is explained in detail as follows:

*3.1.3 Expansion Permutation*

Since the input to the expansion block is 32 bits and the key is 48 bits so we need to expand the input to 48 bits.

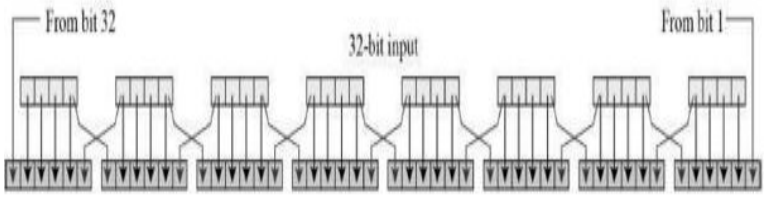


**Figure 5** Graphical Representation of Permutation Logic

*3.1.4 XOR*

After the expansion process, the XOR operation is performed on the expanded key and the round key.

*3.1.5 Substitution-Permutation*

DES with the help of 8 S-Boxes and each S-Box maps a 6-bit input to a 4-bit output.

ISSN:0971-1260
Vol-22- Issue-35-December-2019

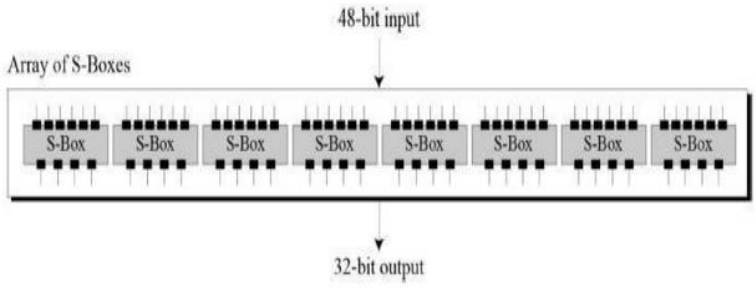


**Figure. 6** S-Box illustrations

*3.1.6 Straight Permutation*

The straight permutation takes the 32-bit input from the substitution-permutation.

The encryption and decryption are the similar processes except the subkeys are inverted in the decryption process. The output of the function is merged with other block and after the last blocks, halves are swapped.

**Algorithm 1** DES Algorithm

---

**INPUT:** G1 . . . ,G64; 64-bit key F=F1 . . . F64 which abide 8 parity bits.

**OUTPUT:** 64-bit ciphertext block C=c1 . . . , c64.

1: Calculate sixteen 48-bit round keys Fi, from F.
2: (L0, T0) <-IP (G1, G2 …G64) with the help of IP Table; divide the result into left and right 32-bit halves L0=G58G50 . . . G8, T0=G57G49 . . . G7)
3: sixteen rounds for i from one to sixteen, calculate Li and Ti as follows:

3.1: Li=Ti-1

3.2: Ti = Li-1 XORf (R i-1, Fi) where f (Ti-1, Fi) = P(S (E (Ti-1) XORFi)), computed as

Follows:

(a)Expand Ti-1 = d1d2 . . . d32 from 32 to 48 bits, T <-E (Ti-1).

(b)H ' <-H XORFi. Represent H ' as eight 6-bit character strings: H '= (A1 . . . A8)

(c)H " <-(S1 (A1), S2 (A2) . . . S8 (A8)). Here Si (Ai) maps to the 4-bit entry in row r and column c of Si

(d)H"' <-P (H"). (Use P per table to permute the 32 bits of H"=h1h2 . . . h32, yielding h16h7 . . . h25.

4: b1b2 . . . b64 <-(T16, L16). (Exchange final blocks L16, T16.)
5: C <-IP-1 (b1b2 . . . b64).
6: End

---

**3.2 Blowfish Algorithm**

Blowfish algorithm has been recognized as the fastest algorithm as compared to DES, AES, and 3-DES in terms of processing time, throughput and execution speed as it makes use of pre-computable subkeys and encrypts data at the rate of 26 clock cycle per seconds. It allows patent free encryption of data and encrypts audio files at slow speed. It takes large blocks for

ISSN:0971-1260
Vol-12- Issue-12-November-2019

manipulating the data. Moreover, it makes use of assorted operations such as modular multiplication, exclusive-or, table lookup and addition. It is composed of two parts:

i. Data Encryption
ii. Key Expansion

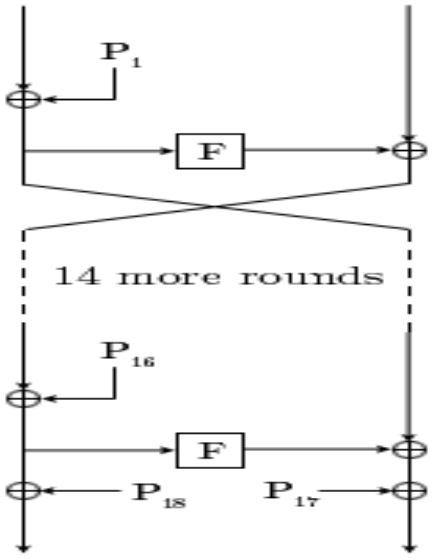


**Figure 7.** The Feistel Structure of Blowfish

*3.2.1 Key Generation*

Blowfish make use of a large number of pre-computed subkeys. It makes use of P-Array and 4 32-bits S-Boxes.

The P-Array comprises of 18, 32-bit subkeys: P1, P2…….P18.

Each W-box include 256 entries:
W1, 0, W1, 1…..W1, 255;
W2, 0, W2, 1…..W2, 255;
W3, 0, W3, 1…..W3, 255;
W4, 0, W4, 1.....W4, 255.

The creation of sub keys using following points:

1. Initialize P-array with S-boxes with the hexadecimal values.

2. XOR include P-array with some key bits recursively one after another as P1 XOR first key, P2 XOR second key and so on.
3. Using the subkeys, in point 1 and point 2 all-zero subkeys are encrypted with Blowfish algorithm.

ISSN:0971-1260
Vol-22- Issue-35-December-2019

4. The output of step 3 is then encrypted using Blowfish algorithm with the modified subkeys.
5. The output of step 5 is then used to add P3 and P4.
6. This procedure is repeated to substitute the value of P-array and S-boxes with the output of ceaselessly varying blowfish algorithm.

*3.2.2 Encryption and Decryption*

The diagram shown below depicts the Blowfish Encryption process. It consists of 18 P-array of 64-bits and 4 S-boxes of 256 entries. Every round includes of four steps: First of all, the data of let half is XORed and the key Kr. The output then acts as input for F-function of blowfish. Then, the output of function f is XORed with the data of the right half. Lastly, the left half and right half is interchanged.

**Algorithm** 2 Blowfish Algorithm

1. begin item
2. The algorithm proceeds for 16 rounds.
3. The input is the plaintext of the 64-bit data element, x.
4. y is splits into two 32-bit halves:
   yR and yL.
5. Then, for z = 1 to 16
   yL = yL XOR Pi
   yR = F (yL) XOR yR
6. Swap yL and yR and after the sixteenth, interchange yL and yR again to undo the last interchange.
7. Now yR = yR XOR P17 and yL = yL XOR P18.
8. At the end, combine yL and yR to get the ciphertext.

ISSN:0971-1260
Vol-12- Issue-12-November-2019

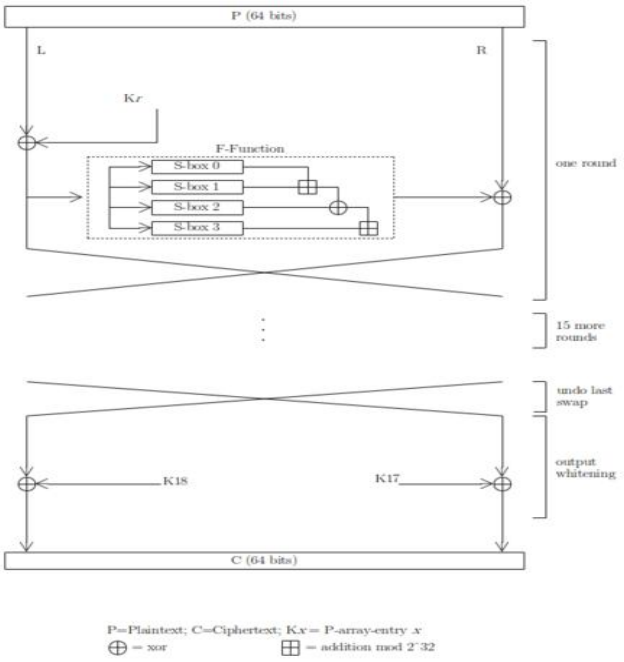


**Figure 8.** Blowfish Encryption

### 3.3. CAST-256 Algorithm

CAST Algorithm is a symmetric block cipher algorithm and the two basic methods for evaluating the security of block cipher algorithm is Differential cryptanalysis and Linear Cryptanalysis. CAST-256 (or CAST-6) algorithm produces a larger output than the input by using the non-bijective S-boxes to controvert to differential cryptanalysis and it also controvert to linear cryptanalysis by developing S-Boxes with bent function.

CAST-256 comprises of six forward quad rounds and six backward or reverse quad rounds. This algorithm works by dividing the n-bit plaintext in 2 halves. The right half $R_i$ along with the key $k_i$ is provided to the round function F for transforming and then the output of function F is XORed bit-by-bit to the left half $L_i$. This procedure is continue for the number of rounds.

$$R_{i+1} = F(R_i, Ki) \cdot \cdot L_i$$
$$L_{i+1} = R_i$$

*3.3.1 Key Generation*

The CAST-256 uses fixed set of round keys. To generate the CAST-256 key schedule an operation known as Octave is used. It is similar to quad round with an exception that it operates on 256-bit block and consists of 8 rounds.

**Algorithm 3 CAST Algorithm**

ISSN:0971-1260
Vol-22- Issue-35-December-2019

**INPUT:** plaintext g1...g64; key F = f1...f128.

**OUTPUT:** ciphertext c1...c64.

1: (Key schedule) Compute 16 pairs of subkeys {Fji, Fri} from F
2: (L0, R0) <-- (j1...j64). (Divide the plain text into left and right 32-bit halves L0 = j1...j32 and R0 = j33...j64.)

3: (16 rounds) for i from 1 to 16, compute Li and Ri as follows: Li = Ri-1; Ri = Li-1 ^ f (Ri-1, Fji, Fri), where f is defined in (f is of Type 1, Type 2, or Type 3, depending on i).

4: z1...z64 <-- (R16, L16). (Exchange final blocks L16, R16 and concatenate to form the ciphertext.)

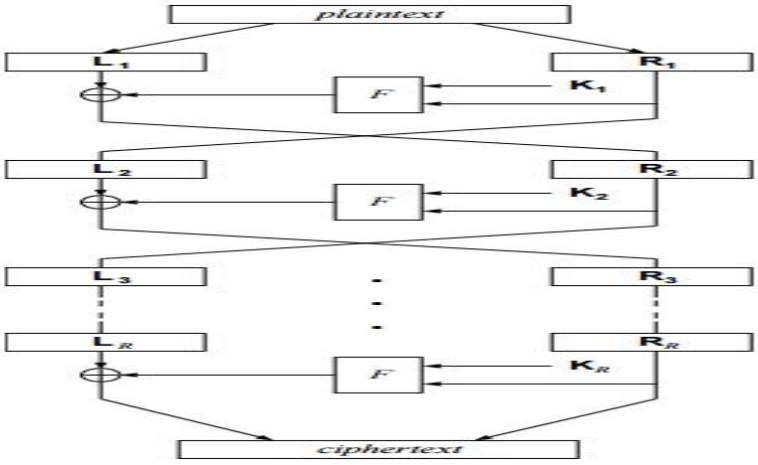


**Figure 9.** CAST Encryption Algorithms

## 4. PROPOSED WORK

As the data security threats are increasing these days so to combat them a technique has been proposed in this paper which provides security by key generation process in the first phase. The keys such as secret key, sharing key, OTP, and Identification key are generated and by use of these keys, security is provided for the cloud storage. In the second phase, encryption and decryption process takes place in which the file which is stored by the user on storage is encrypted by using DES, CAST, DES-CAST, BLOWFISH and DES-BLOWFISH algorithm. The analysis results show that execution time of DES with BLOWFISH is lesser than other algorithms and complexity of DES with BLOWFISH is higher than other algorithms.

## 5. EXPERIMENTAL SETUP

ISSN:0971-1260
Vol-12- Issue-12-November-2019

JAVA has been used for implementation and Cloud Sim (Wang, 2009) its package and Jar files for implementing the proposed algorithm. The data of the software engineering book (Sommerville, 2010) is taken as plain text input as shown in fig 10 and the output after encrypting the file with DES, CAST, DES-CAST, BLOWFISH, and the DES-BLOWFISH algorithm is shown in fig 11.
Performances of these five algorithms were measured on Intel Core i3 @ 2.90 GHz 32-bit operating system with 4 GB of RAM running windows 7 ultimate.

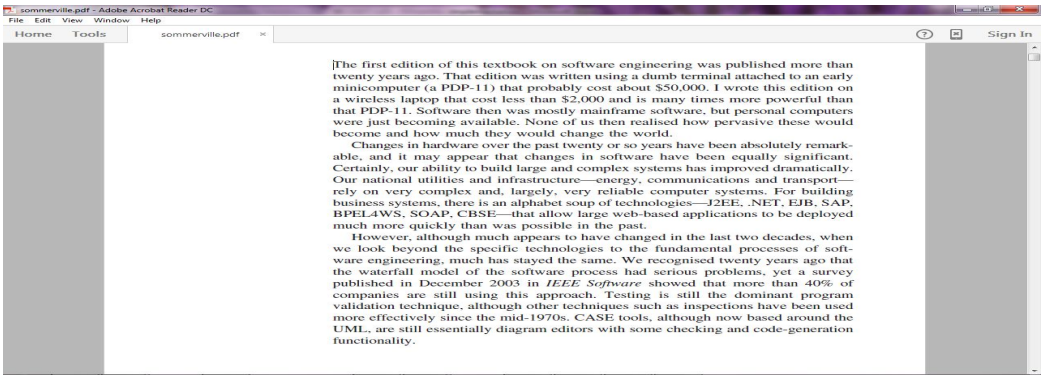


**Figure 10** Plain Text Input File (.pdf)

ISSN:0971-1260
Vol-12- Issue-12-November-2019

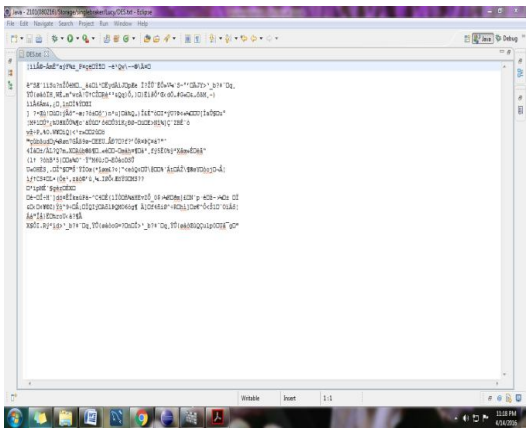

**Figure 11.1** Cipher Text Output (DES)

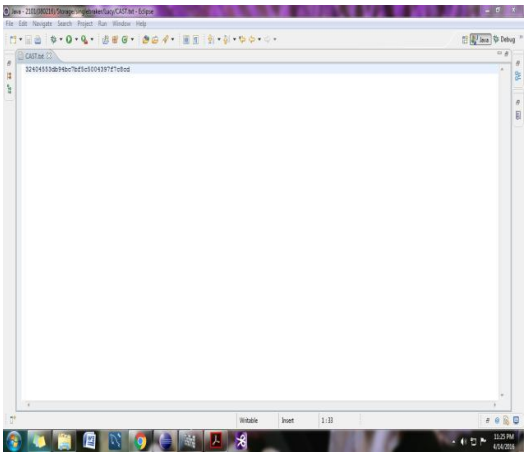

**Figure 11.2** Cipher Text Output (CAST)

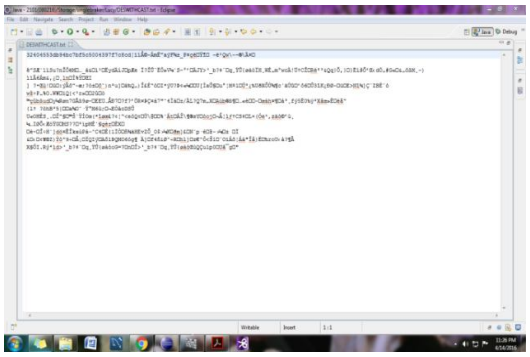

**Figure 11.3** Cipher Text Output (DES-CAST)

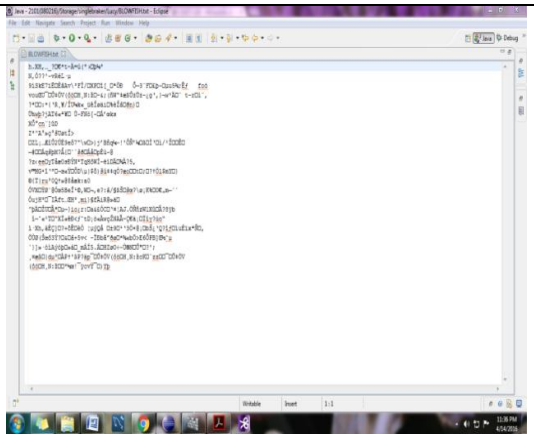

**Figure 11.4** Cipher Text Output (BLOWFISH)

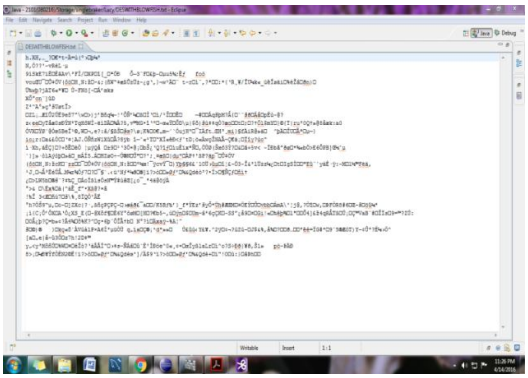

**Figure 11.5** Cipher Text Output (DES-BLOWFISH)

ISSN:0971-1260
Vol-12- Issue-12-November-2019

## 6. PERFORMANCE AND ANALYSIS

The proposed algorithm proves to be better in terms of execution time and complexity when executed with different file sizes which are depicted in Table 1.

**Table 1** Execution Time Vs Complexity

| Algorithms | File Size (in bytes) | Execution Time | Complexity |
|---|---|---|---|
| DES | 792 | 0.0631565 | 3961.584 |
| CAST | 32 | 1.5631249 | 160.064 |
| BLOWFISH | 792 | 0.0631565 | 3961.584 |
| DES-CAST | 824 | 0.0607038 | 4121.648 |
| DES-BLOWFISH | 1584 | 0.0315782 | 7923.168 |

### 7.1 Performance Comparison

*7.1.1 Execution Time*

The Graph shown below depicts that the execution time of DES with Blowfish is lesser than the other algorithms.

ISSN:0971-1260
Vol-12- Issue-12-November-2019


**Figure 12** Execution Time of Different Algorithms

*7.1.2 Complexity*

The Graph shown below depicts that the complexity of DES with Blowfish is higher than other algorithms.

**Figure 13** Complexities of Different Algorithms

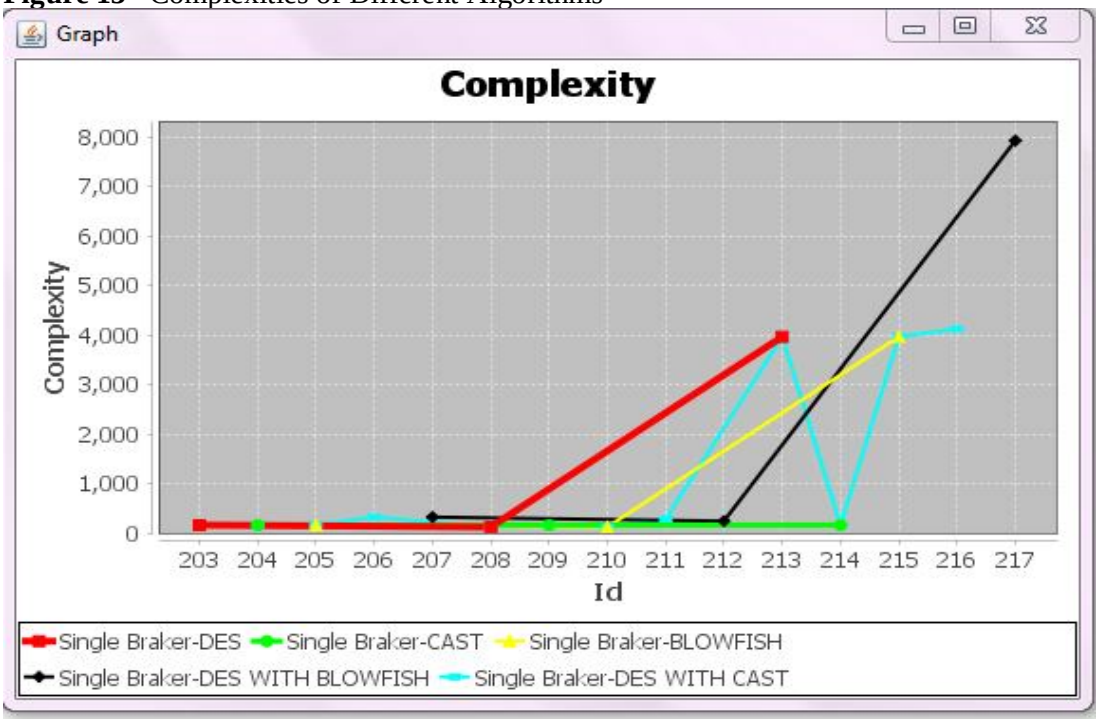


**Figure 13** Complexities of Different Algorithms

## 8. CONCLUSION

ISSN:0971-1260
Vol-12- Issue-12-November-2019

In this paper, DES, CAST, BLOWFISH, DES-CAST, DES-BLOWFISH algorithms were compared in terms of execution time and complexity. These algorithms can be applied to any data which includes text, images, and audio of any size.

Firstly, the paper is focused on reducing the execution time of the algorithm so that it can provide the results of encryption must faster than other algorithms and secondly, to increase the difficulty of the algorithm so that it should not be hacked easily. In this paper, these have been achieved by hybrid algorithms.

With data encryption, the client can also access other facilities by providing identification key which includes viewing the stored files in the cloud server with certain attributes such as file size, access modes and when the file was last modified, downloading the file to cloud storage and storing the file into cloud storage. On the other hand, only the authorized client can access these services and encrypt the data on a cloud server.

Results conclude that performance of DES and CAST is same when applied individually and the performance of DES with BLOWFISH is better than the DES with CAST.

**REFERENCES**

[1] C. Adams and J. Gilchrist, "The CAST-256 Encryption Algorithm", Vol. 12, pp.71–104. 1999.

[2 ]J. Aggarwal, "Performance Evaluation of RC6, Blowfish", DES, IDEA, and CAST-128 Block Ciphers', Vol. 68, No.25, pp.10–16,2013.

[3] A. Alabaichi and F.Ahmad, "Security analysis of blowfish algorithm", *2nd International Conference on Informatics and Applications, ICIA* , pp.12–18,2013.

[4] M. Armbrust et al. "Above the clouds: A Berkeley view of cloud computing", *University of California, Berkeley, Tech. Rep. UCB,* pp.07–013,2009

[5] A.Behl, "An analysis of cloud computing security issues",*World Congress on* Information *and Communication Technologies (WICT),* pp.109–114,2012.

[6] R.Buyya and J.Brober, "*Cloud Computing: Principles and Paradigms"*, New York: John Wiley and Sons,2011.

[7] C. Czarnecki, "Cloud Computing Promises : Fact or Fiction. *Computing"*2013.

[8] D.Zien, "Addressing cloud computing security issues", *Future Generation Computer Systems,* Vol. 28, No.3, pp.583–592, 2012.

[9] A.K Dubey et al. "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment", *CSI 6th International Conference on Software Engineering, CONSEG, 2012*.

[10]Fatemi Moghaddam and Karimi, "A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments", *2nd International Conference on Cloud Networking (CloudNet),* pp.185–189,2013.

 

ISSN:0971-1260
Vol-12- Issue-12-November-2019

[11] H.Feistel,'Data Encryption Standard (Des)', *Federal Information Processing Standard ,Pub 46-3*,2011.

[12] H.M Heys and S.E Tavares, "On the Security of the CAST Encryption Algorithm", *Canadian Conference on Electrical and Computer Engineering*, pp.332–335,2000.

[13] H.Y.Lin and W.G Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 6, pp.995–1003,2012.

[14]Tutorial Point. Available at: http://www.tutorialspoint.com/cryptography/data_encryption_standard.htm.

[15] A.Moussa, "Data encryption performance based on Blowfish", 47th *International Symposium ELMAR*, pp.131–134, 2015.

[16] T.Nie and T.Zhang, "A study of DES and blowfish encryption algorithm", *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, pp.1–4,2013.

[17] K. Popovićand Z. Hocenski, "Cloud computing security issues and challenges", pp.344–349,2010.

[18] M.Prakash and Parteek Singh, "Data encryption and decryption algorithms using key rotations for data security in cloud system", *2014 International Conference on Signal Propagation and Computer Technology, ICSPCT 2014*, Vol. 3, No.4, pp.624–629,2014.

[19] B. Schneier "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", In *Cambridge Security Workshop Proceedings , Springer-Verlag*. pp. 191–204,2017.

[20]J.Y Zha and L. Wen, "Improved Linear Cryptanalysis of CAST-256", Journal *of Computer Science and Technology*, Vol. 29, No. 6, pp.1134–1139,2014.