Secure Data Sharing using Data Encryption Standard in Cloud

Nara Kalyani[1] Ms C Yamini[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Applications
[1,2]KMM Institute of PG Studies, Tirupati, India

Abstract— The vital objective managing the plan of any encryption calculation must be security against unapproved assaults. Inside the most recent decade, there has been a huge increment in the collection and correspondence of computerized PC information in both the private and open divisions. A lot of this data has a noteworthy esteem, either straight forwardly or in a roundabout way, which requires security. The calculations extraordinarily characterize the numerical advances required to change information into a cryptographic figure and furthermore to change the figure back to the first frame. Execution and security level is the primary attributes that separate one encryption calculation from another. Here acquaints another technique with improve the execution of the Data Encryption Standard (DES) calculation is presented here. This is finished by supplanting the predefined XOR task connected amid the 16 round of the standard calculation by another activity relies upon utilizing two keys, each key comprises of a mix of 4 states (0, 1, 2, 3) rather than the conventional 2 state key (0, 1). This substitution includes another dimension of assurance quality and more vigor against breaking techniques.

Keywords: DES, Encryption, Decryption

I. INTRODUCTION

Cryptography is typically alluded to as the investigation of secret‖, while now a days is most joined to the meaning of encryption. Encryption is the way toward changing over plain content unhidden‖ to an enigmatic content hidded to anchor it against information criminals. This procedure has another part where enigmatic content should be unscrambled on the opposite end to be comprehended in figure 1.

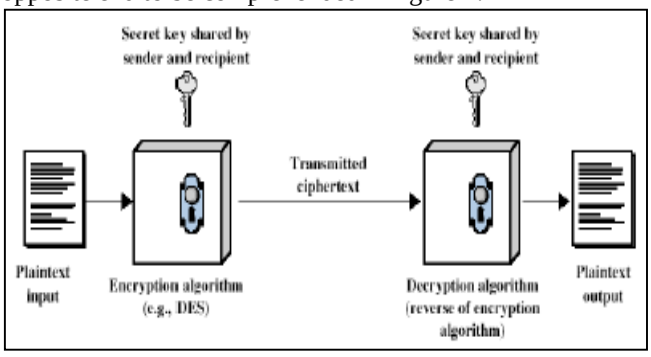


Fig. 1: Encryption/Decryption

A. *Cryptography Goals: [2]*

1) Privately: Information in PC transmitted data is available just to peruse by approved gatherings.
2) Confirmation Origin of message is effectively related to an affirmation that character isn't false.
3) Trustworthiness Only approved gatherings can alter transmitted or put away data.
4) Non Repudiation-Requires that neither the sender, nor the beneficiary of message have the capacity to deny the transmission.
5) Access Control-Requires access might be controlled by or for the objective framework.
6) Accessibility Computer framework resources are accessible to approved gatherings when required.

II. INFORMATION ENCRYPTION STANDARD

Without uncertainty the first and the most noteworthy current symmetric encryption calculation is that contained in the Data Encryption Standard (DES).The DES was distributed by the United States' National Bureau of Standards in January 1977 as a calculation to be utilized for unclassified information (data not worried about national security). The Data Encryption Standard (DES), as indicated in FIPS Publication 46-3, is a square figure working on 64-bit information squares. The encryption change relies upon a 56-bit mystery key and comprises of sixteen Feistel emphasess encompassed by two stage layers: an underlying piece change IP at the info, and its backwards IP−1 at the yield. The structure of the figure is delineated in Figure 2. The decoding procedure is equivalent to the encryption, aside from the request of the round keys utilized in the Feistel iterations.[12] The 16-round Feistel arrange, which establishes the cryptographic center of DES, parts the 64-bit information obstructs into two 32-bit words, LBlock and RBlock (indicated by L0 and R0). In every emphasis (or round), the second word Ri is encouraged to a capacity f and the outcome is added to the main word Li. At that point the two words are swapped and the calculation continues to the following emphasis. The capacity f of DES calculation is key ward and comprises of 4 phases.

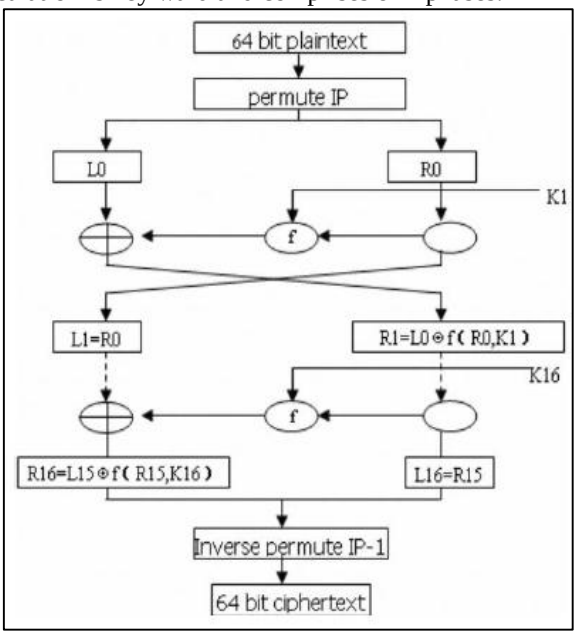


Fig. 2: DES Algorithm

A. *Extension (E):*

The 32-bit input word is first extended to 48 bits by copying and reordering half of the bits.[11]

B. Key Blending:

The extended word is XORed with a round key developed by choosing 48 bits from the 56-bit mystery key, an alternate choice is utilized in each round.

C. Substitution:

The 48-bit result is part into eight 6-bit words which are substituted in eight parallel 6×4-piece S-boxes. Every one of the eight S-boxes, are extraordinary yet have a similar exceptional structure.

D. Change (P):

The subsequent 32 bits are reordered by a settled stage before being sent to the yield. The changed RBlock is then XORED with LBlock and the resultant nourished to the following RBlock register. The unmodified RBlock is sustained to the following LBlock enlist. With another 56 bit subordinate of the 64 bit key, a similar procedure is rehashed.

Pseudo Code : Data Encryption Standard
INPUT : plaintext m1 . . . m64; 64-bit key K=k1 . . . k64 (includes 8 parity bits).
OUTPUT : 64-bit ciphertext block C=c1 . . .c64.
1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
2. (L0, R0) ← IP(m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:
3.1. Li=Ri-1
3.2. Ri = Li-1 XOR *f* (R i-1, Ki)
where *f*(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:
(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits, T ←E(Ri-1).
(b) T ' ←T XOR Ki. Represent T ' as eight 6-bit character strings: T '= (B1 . . . B8)

(c)T '' ←(S1(B1), S2(B2), . . . S8(B8)). Here Si(Bi) maps to the 4-bit entry in row r and column c of Si
(d)T''' ←P(T''). (Use P per table to permute the 32 bits of T''=t1t2 . . . t32, yielding t16t7 . . . t25.)
4. b1b2 . . . b64 ← (R16, L16). (Exchange final blocks L16, R16.)
5. C ← IP-1 (b1b2 . . . b64).
6. End.

Algorithm 1. DES Algorithm

III. ENHANCED 4 STATE OPERATIONS

To expand the security and key space, that makes the encryption calculations more vigor to the interlopers, another control bits process has been included by utilizing diverse truth table for control bits process chip away at 4-states (0,1,2,3) , while the customary double process (XOR) take a shot at (0, 1) bits as it were. The image # has been utilized to allude to the administrator that execute this procedure use truth tables that appeared in figure 3.[7]

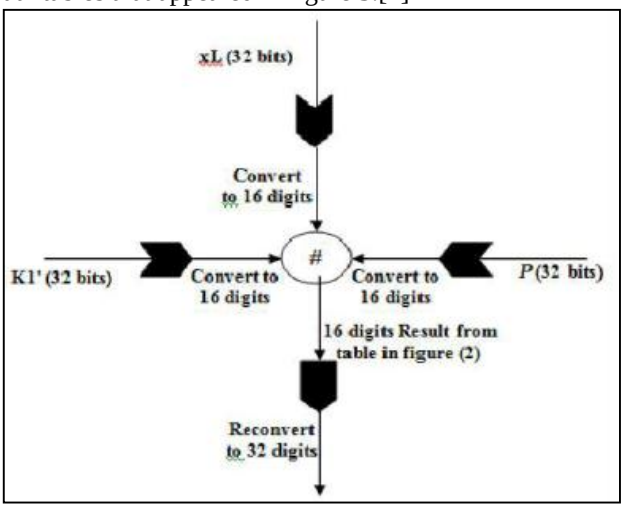


Fig. 3: Design of Modified DES Algorithm

The new task needs 3 inputs, the first indicate the table number that ought to be utilized to figure the outcome among the 4 tables, the other 2 inputs characterize the line and section number in the predefined table where the cross purpose of them gives the outcome. Here, case for # activity, this task require 3 inputs, initial one determine the table number that ought to be utilized to figure the outcome among the four truth tables as appeared Table 1, the other 2 inputs characterize the line and section number in the predefined table where the cross purpose of them gives the outcome this outcome is in 16 digits. Contribution to 32 bit parallel arrangement 10010111010100101010011111010001001 which is changed over into the number

2 1 3 1 0 2 1 3 2 0 2 1
Input 1: 0 1 3 0 1 2 3 1
Input 2: 3 2 1 0 1 2 1
Input 3: 1 0 2 1 3 2 1 2
Result : 3 0 2 3 1 2

#0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

#2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

#3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

Table 1: Truth Table

IV. PROPOSED ALGORITHM OF DES

This exploration proposed another enhancement to the DES calculation. The proposed enhancement makes utilization of

the new task characterized in the past area, activity (#) connected amid each round in the first DES calculation, where another key is expected to apply this activity, this key may come in paired frame and convert to a 4-states key. Here, initially DES calculation direct cryptanalysis and differential cryptanalysis assaults are vigorously relies upon the S-box plan. Therefore, different keys will be utilized in each round of the first DES, the primary key Ki will be utilized with the f work. The second key will be the principal contribution to the # task, the second information will be the yield of the f work, and the third contribution to the # activity will be the esteem Li, Algorithm demonstrates the three 32-bits contribution to the # task ,and the 32-bits yield, with spots expected to change over these 32-bits to 16-digits. These three contributions to the # task ought to be initially changed over from 32 bits to a 16 digits each might be one of four states (0,1,2, 3), i.e., every two bits changed over to its proportional decimal digits. Calculation of altered information encryption standard with 4 state tasks:

INPUT : plaintext m1 . . . m64; 64-bit two keys K=k1 . . . k64 and K'=k1' . . . k64' (includes 8 parity bits).
OUTPUT : 64-bit ciphertext block C=c1 . . .c64.
1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
   1.1. (key schedule) compute sixteen 32-bit round keys Ki', from K'
2. (L0, R0) ← IP (m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:
   3.1. Li=Ri-1
   3.2. Ri = Li-1 # *f* (R i-1, Ki)
where *f*(Ri-1, Ki) = P(S(E(Ri-1) Å Ki)), computed as follows:
   (a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits T ← E(Ri-1). (Thus T= r32r1r2 . . . r32r1.)
   (b) T' ← T XOR Ki . Represent T ' as eight 6-bit character strings: T ' = (B1 . . . B8)

(c)T " □ F where Function F = (((((((S1+S2) mod 2 ^ 32) XOR S3) + S4) mod 2^32) XOR S5) +S6)mod 2^32 Here, Si(Bi) maps to the 8 bit passage in line r and segment c of Si (d)T'" □ P(T"). (Use P per table to permute the 32 bits of T"=t1t2 .. ... … . t32,yielding t16t7 . . . t25.) and the activity # in Ri = Li-1 # f (R I-1, Ki) is registered as pursues: (I)Convert the 32 bits came about because of f (R I-1, Ki) into 4-states 16 digits call it f ' (II) Convert the 32 bits of Li-1 to 4-states 16 digits call it Li-1' (III) Convert the 32 bits of Ki' to 4-states 16 digits call it Ki" (IV) Compute Ri by applying the # task on f ', Li-1', and Ki" as indicated by truth tables appeared Table.
4. b1b2 . . . b64 □ (R16, L16). (Trade last squares L16, R16.)
5. C □ IP-1 (b1b2 . . . b64). (Transpose utilizing IP-1 C = b40b8 . . . b25.)
6. End. Calculation 2 Modified DES Algorithm

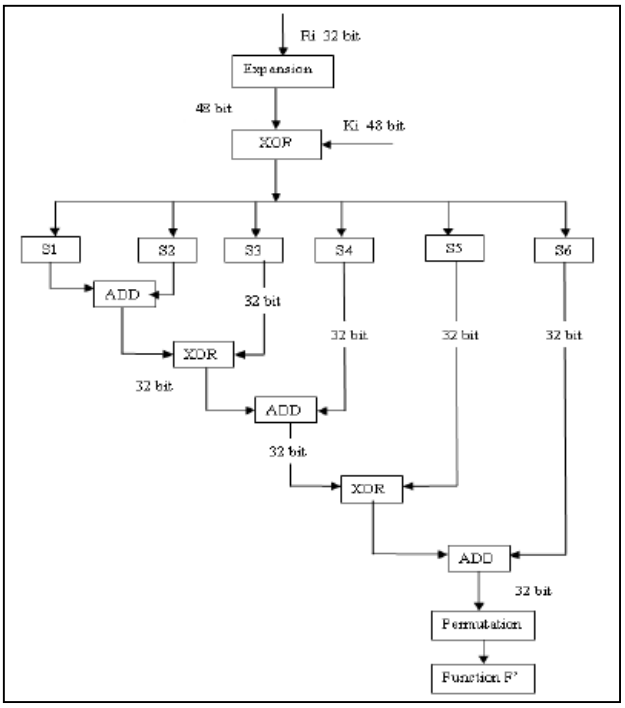


Fig. 4: Function F Design

Here, utilizing this proposed calculation fathom model. Our Input Message is 0123456789ABCDEF which is our plain content is changing over into figure content utilizing this proposed calculation. Here, There are 16 rounds for believer plain content to figure content. In each round it contain two keys, change of 16 bit information to 32 bit information and the other way around. First we convert plain content into double arrangement likewise we need to change over key into twofold organization which is additionally in hex configuration. Presently, playing out all activity of this proposed calculation and get the figure content. Capacity F we need to given 8 bit input utilizing that input we got 32 bit o/p from the s-box and perform XOR task and ADD activity.

1) Step 1: Create Subkeys: K1 to K16 Key =133457799BBCDFF1
2) Step 2: Initial Permutation of Message which is given by User.
3) Step 3: for I =1 to 16 round Ln = Rn-1 Rn = Ln-1 # f(Rn-1,Kn)
4) Step 4: Convert 16 bit information into 32 bit information. After total one round we got

F' = 11 33 22 03 01 03 33 02
L' = 30 00 30 33
K' = 31 12 13 20 21 13 20
R1= 31 01 20 02 12 13 01 12

Here,R1 esteem discovered utilizing truth table and got 16 bit information that is changed over into 32 bit information.

R1 = 1101 0001 1000 0010 0110 0111 0001 0110

After finishing each of the 16 round we got L16R16 esteem.

L16: 0000 1011 0011 1110 1010 1001 0100
R16 : 1111 0010 0111 0000 0110 1111 0100
R16 L16 = 1111 0010 0111 0000 0110 1111 0100 0000 1011 0011 1110 1010 1001 0100

Now, Inverse of IP has been performed:

IP-1: 1010 0000 1110 1100 0000 0111 1000

0111 0001 0111 1001 0101 101 0100 1011

So, at last we got our figure content A0EC07887178594B Now, contrast this arrangement and our unique des calculation we got torrential slide impact and furthermore illuminate cryptanalysis assault.

V. RESULT AND ANALYSIS

A. *CSP-login*

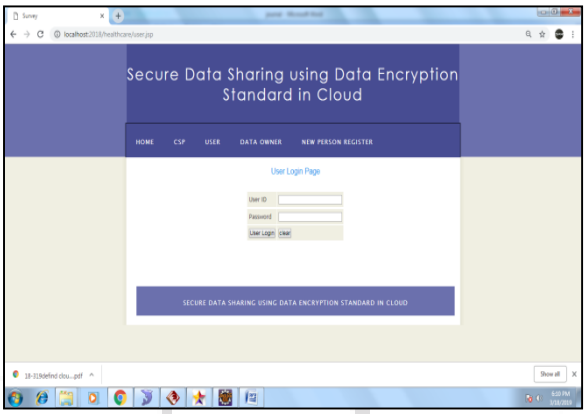
B. *View Users*

C. *View Owners*

D. *View Requests*

E. *User/Owner Registration*

F. *User Login*



G. *View Files*

H. *View Response*

I. Data Owner Login

J. Data Owner Home

K. Upload Files

L. View Requests

VI. CONCLUSION

As we toward a general public where computerized data assets are expanded and cryptography will keep on expanding in significance as a security instrument. Electronic systems for saving money, shopping, stock control, advantage and administration conveyance, data stockpiling and recovery, dispersed handling, and government applications will require enhanced strategies for access control and information security. The data security can be effectively accomplished by utilizing Cryptography strategy. DES is presently viewed as uncertain for a few applications like managing an account framework. there are likewise some explanatory outcomes which exhibit hypothetical shortcomings in the figure. So it turns out to be imperative to increase this calculation by adding new dimensions of security to make it relevant. By including extra key, altered S-Box configuration, alters work usage and supplanting the old XOR by another activity as proposed by this theory to give more power to DES calculation and make it more grounded against any sort of meddling. DES Encryption with two keys rather than one key as of now will build the effectiveness of cryptography.

REFERENCES

[1] Tingyuan Nie, Teng Zhang ― A Study of DES and Blowfish Encryption Algorithm‖,TENCON, 2009
[2] Afaf M. Ali Al- Neaimi, Rehab F. Hassan ― New Approach for Modified Blowfish Algorithm Using 4 – States Keys‖ , The 5th International Conference On Information Technology,2011
[3] J.Orlin Grabbe ―The DES Algorithm Illustrated‖
[4] Dhanraj, C.Nandini, and Mohd Tajuddin An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard‖, International Journal of Research And Review in Computer Science, August 2011
[5] Gurjeevan Singh, Ashwani Kumar, K.S. Sandha ―A Study of New Trends in Blowfish Algorithm ‖, International Journal of Engineering Research and Application,2011
[6] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.
[7] B.Scheier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd ed.., John Wiley & Sons, 19995.
[8] National Bureau of Standards – Data Encryption Standard, Fips Publication 46, 1977.
[9] O.P. Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi ― Performance Analysis Of Data Encryption Algorithms ― , 2011
[10] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha ― Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2011.
[11] Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound ― Performance Evaluation of Symmetric Encryption Algorithm ―, IJCSNS, 2008
[12] Dr. Mohammed M. Alani ― Improved DES Security‖ , International Multi-Conference On System, Signals and Devices, 2010

