International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-6, May 2023

Improved Data Encryption Standard Algorithm using Zigzag Scan for Secured Data Transmission

S. Hemasri, S. Kiran, A. Ranichitra, A. Rajesh Kanna

***Abstract:** The cryptosystem is a combination of cryptographic algorithms used to provide security services for the information. One of them is the data encryption standard also known as DES which is a symmetric-key block cipher released by national bureau of standard (NBS). DES is a block cipher and perform encryption of each block of size 64 bits. Encryption of the data by using an algorithm which translates the original data into an unreadable format which is not easy for the intruder to attack. The DES is secure than the other cryptosystems, because the time required for processing cryptanalysis has minimized and because of the development in the hardware technique, the traditional DES may be unsafe by different kinds of attacks by the different cryptanalysis. This paper implements a new design of DES called the Improved DES which exhibits that the improved DES is secure than the DES against differential cryptanalysis. It divides each substitution box into four sub blocks of 16 bits and then executes the zig-zag function of each of the 4-sub blocks. It improves the standard encryption levels by columnar transposition.*

***Keywords:** Cryptography, DES, Zigzag Scan, Key Generation.*

I. INTRODUCTION

Now-a-days data becomes the biggest resource for every organization either it is confidential or non-confidential. It is the major challenge for the organization to provide security for the data which is confidential i.e., the data is not shared with others. Different kind of attacks on major organizations aims for stealing of data. Therefore, providing security is the major concern.

A. Cryptography

Cryptography is all about the techniques supporting private and secure communications. It attempts to preserve the integrity of data and curb snoops from reading it. It is the study of techniques and procedures used to secure information by making it unreadable to unintended recipients. Here are some cases where cryptography played a significant role in protecting your communication:

Manuscript received on 04 April 2023 | Revised Manuscript received on 25 April 2023 | Manuscript Accepted on 15 May 2023 | Manuscript published on 30 May 2023.
*Correspondence Author(s)

S. Hemasri*, Ph.D (Pursuing), Department of Computer Science, Madurai Kamraj University, Madurai (Tamil Nadu), India. E-mail: hema0129@gmail.com, ORCID ID: https://orcid.org/0009-0001-6103-0276

Dr. S. Kiran, Associate Professor, Department of Computer Science and Engineering, Yogi Vemana University, Ganganapalle (A.P), India. ORCID ID: https://orcid.org/0000-0002-0725-3356

Dr. A. Ranichitra, Assistant Professor, Department of Computer Science, S.Ramasamy Naidu Memorial College, Sattur (Tamil Nadu), India. ORCID: https://orcid.org/0000-0001-6071-0635

Dr. A. Rajesh Kanna, Assistant Professor, Department of Computer Science, S.Ramasamy Naidu Memorial College, Sattur (Tamil Nadu), India. ORCID: https://orcid.org/0000-0001-5161-4334

- Logged in to your account by providing your credentials.
- Bought something online through your credit card.
- Sent a message to your friend through instant messaging platforms.

B. Public Key Cryptography

The public key cryptography or asymmetric cryptography works on set of keys. public key and private key in order to encrypt the data sender use the receiver's public key and to decrypt the data uses receiver's private key.

RSA (Rivest, Shamir, Adelman) And DSA (Digital Signature Algorithm) are the two different types of public key cryptography algorithms. By using PKC confidentiality can be provided that is to perform encryption sender has to use receiver's public key and to decrypt receiver use the unique private key ensure that no other person can decrypt the data.

C. Private Key Cryptography

Private key encryption uses the same key for both encryption and decryption. Encryption and decryption process may lead to the key management issue. The main drawback of secrete key cryptography is protecting the key when everyone is using private key.

For example, if a user wants to communicate with different people must uses different private keys. For a group of N people, it will make use of keys equal to N*(N-1)/2.

D. Methods of Cryptography

- Symmetric Cryptography
- Asymmetric Cryptography
- Hashing

a. Symmetric Cryptography

In symmetric cryptography both the sender and receiver use a common secrete key to share encrypted data i.e., symmetric encryption utilizes a key to encrypt the plain text into cipher text and transfer it to receiver where the receiver also applies the same key to decrypt the cipher text into plain text.

In the block algorithms the length of bits is encrypted in blocks another one is stream algorithms where the data is encrypted in the form of streams are the two types of symmetric cryptography algorithms. Some of the symmetric encryption algorithm examples are AES, DES, IDEA etc.,

b. Asymmetric Cryptography

Public key cryptography or asymmetric cryptography works on pair of keys – public key and private key to preserve data from the unauthorized access. The data should be encrypted with the public key but the cipher text can be decrypted only with the intended recipient private key.

In order to establish a secure connection between two parties this asymmetric encryption process is also used. It is also used to establish encrypted links between websites and browsers in SSL (Secure Socket Layer) and TLS (Transport Layer Security). Examples of Asymmetric cryptography are ECC (Elliptic Curve Cryptosystem), DSS (Digital Signature Standard).

c. Hashing

Algorithm that considers arbitrary amount of input data and generates an encrypted text of fixed size is called a hash value. Hashing is a mathematical operation of cryptography that transforms data into string of text. Hashing is easy to execute but immensely difficult to reverse. Some of the hashing algorithms are MD5 (Message Digest5), SHA1 (Secure Hashing Algorithm1), SHA256.

E. Decryption Process

The decryption process is just the reverse of encryption process which converts the received cipher text into plain text.

II. LITERATURE SURVEY

- Sombir Singh Et Al [1] proposes a secure communication system which uses a private key cryptography-Data encryption standard (DES). Before the implementation of DES algorithm a transposition technique is added to improve the security of DES algorithm. Security has been improved which is prominent in the field of communication using the proposed method. While implementing the transposition technique, the attacker initially needs to break the main DES algorithm and then transposition technique.
- Nirmaljeet Kaur and Sukhman Sodhi [2] identifies substitution(confusion) and transposition(diffusion) based on DES is implemented. Some of the online applications like banking system etc are considered to be unsecure to perform encryption using DES. In this paper few analytical results which represents theoretical weaknesses in the cipher. Therefore, to maximize the standard DES algorithm, new level of security is added to it.
- Na Su Et Al [3] proposed paper optimizes the AES algorithm and combines the characteristics of IoT computing resources and storage resources to construct the data encryption standard DESI in the Internet of Things. This paper creates the data encryption standard DESI in the Internet of Things depend on the AES algorithm and shows that DESI has higher efficiency than the AES algorithm. Incorporated with the security analysis of DESI, it can be proved that DESI merges efficiency and security, and is useful for providing encryption protection for the data in the IoT environment.
- Wang sheng and Zhou Jian [4] proposes higher requirements for the security protection technology of information communication. The 3DES algorithm is produced after three rounds of polling based on the DES algorithm, which uses shift, XOR, S-box and other operations. The conclusion was the information communication data encryption technology proposed in the paper and traditional encryption technology are compared and tested in terms of encryption strength, data processing efficiency and encryption and decryption time.
- Khalid Ali Hussein Et Al [5] proposed method was a parallel environment has been utilized to construct a new encryption system, based on involving the so-called 'zig-zag' ordering that is used in JPEG data compression. A new chaotic system of three dimensions is generated to remove the regular encryption problems.
- Pratibha Chaudhary Et Al [6] identifies that the proposed work is implemented on grayscale images applied on MATLAB version 2016a. The experimental results exhibits that the proposed work provides good compression ratio. Ultimately a joint image compression and encryption work proposed for a grayscale image with various dimensions like 256X256, 512X512 and 1024X1024 and of different sizes.
- Li, S., Zhao, L., & Yang, N. [7] offers a secure triple layer image steganography technique works on zigzag pattern for embedding secret data. This paper uses a triple layer message security scheme, where the initial two layers based on cryptographic function and the third layer is based on steganographic function. The encrypted bits are enabled within the LSBs of each with the R, G and B color channels applies a zigzag pattern to identify the order in which the encrypted bits are organized.
- Ahmed A. Abd El-Latif Et Al [8] proposes a conventional method for cryptographic techniques depend on mathematical computation-based construction. Quantum walks (QWs) is a universal quantum computational model, which compromises of inherent cryptographic features ply to build efficient cryptographic mechanisms. This paper utilizes the features of quantum walk to generate a new S-box method which plays a prominent role in block cipher techniques for 5G-IoT technologies.
- Shanshan Li Et Al [9] identifies an algorithm works on a chaotic system constitutes the two-dimensional Sine Logistic modulation map (2D-SLMM) and the two-dimensional Hénon-Sine map (2D-HSM). The encryption method is made up of zigzag scan scramble, pixel grey value transformation, and dynamic diffusion. The pixel grey value transformation uses a password feedback method. The proposed work is lossless for medical image encryption and decryption. The problems of low-dimensional chaotic map such as narrow interval and some parameters, besides with the problem of the spectral texture and contour of medical images are avoided.
- Harshali D. Zodpe Et Al [10] proposed method presents a low-cost Field Programmable Gate Arrays (FPGA's), builds special purpose hardware for computationally intensive applications which became feasible. This paper presents the design for Hardware implementation of Data Encryption Standard (DES) based on FPGA applies an exhaustive key search. Iterative and Loop unrolled DES architecture are implemented in this paper.

- Mohit Agarwal [11] proposes a Format Preserving Encryption method achieved with the help of exclusive OR operation, Advance encryption standard (AES), and a translation method for 16-digit numeric data. In order to minimize the databases modifications by securing the length and format of input data the format preserving encryption method is used. The defects which occur in the proposed method like prefix schemes, length preserving encryption mechanism and cycle walking are overcome using this method.
- Ali Mohammed Ali Argabi and Md Imran alam [12] identifies an integrated concept DES and AES Algorithms and generates a new algorithm like AEDS. It is tested with various inputs like files and strings (AES, DES and AEDS) on three different Machines. AEDS Algorithm shows best results over the two Algorithms because it defeats the drawbacks of that algorithms. Brute force attack is minimized as compared to the rest two algorithms.

III. DATA ENCRYPTION STANDARD

A. Introduction

The Data Encryption Standard is used to preserve digital data. Encryption process translates the plain text into cipher text. Decryption process converts the cipher text into the original plain text.

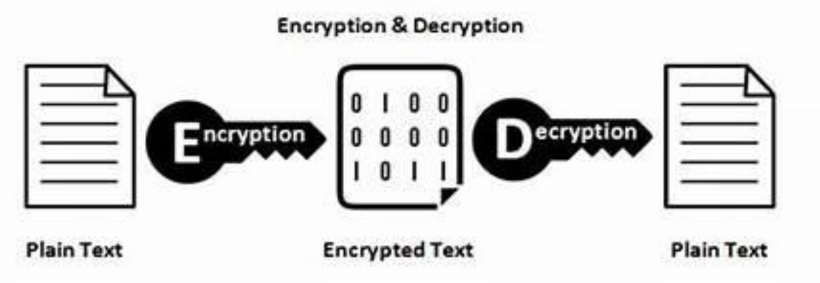

Figure 1: Over all representation of Encryption and Decryption

DES accept input of 64 bits and the output is also of the similar size. A secret key with a length of 64 bits is considered as a second input. It uses a Block cipher algorithm, divides the message into blocks of bits. These blocks of bits passed through substitution, transposition, and other different mathematical functions [1].

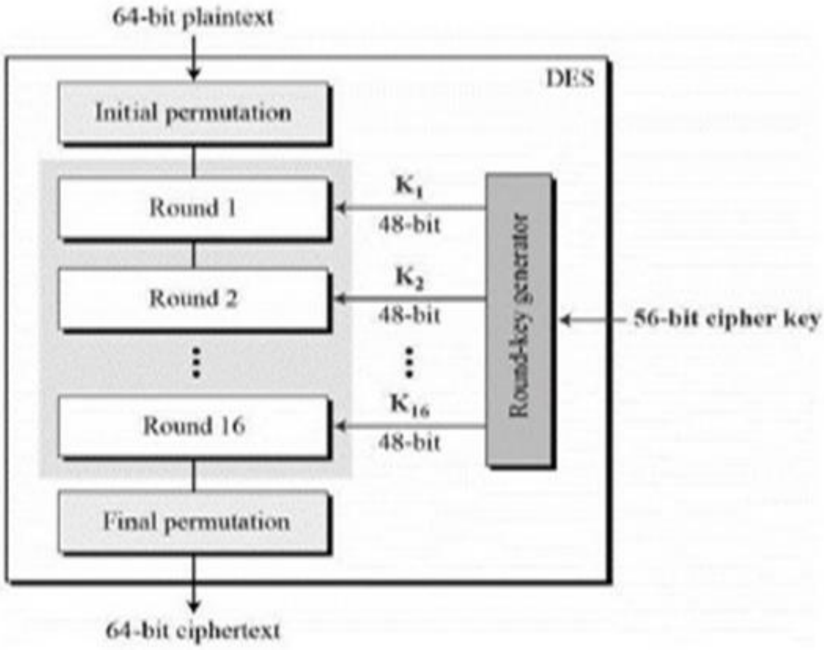

Figure 2: Representation of DES

B. Data Encryption Standard Algorithm

The standard algorithm used by the DES to perform encryption and decryption process as follows,

DES Algorithm Steps

DES uses 64-bit plain text and transform it into a 64-bit ciphertext. The algorithm process uses the following steps [2]:

1. Initially a 64-bit plain text will be accepted and transferred it to the initial permutation round.
2. The initial permutation rearranges the bits into two portions, named as left and right.
3. During the encryption process both the left and right portions go through 16- rounds.
4. At last, the two portions are merged, we get a final permutation.
5. Finally, a 64-bit ciphertext is generated using above steps.

C. Initial and Final Permutation

The initial and final permutations are keyless straight permutations which are reverse to each other [3]. The below figure shows some of the inputs and their equivalent outputs

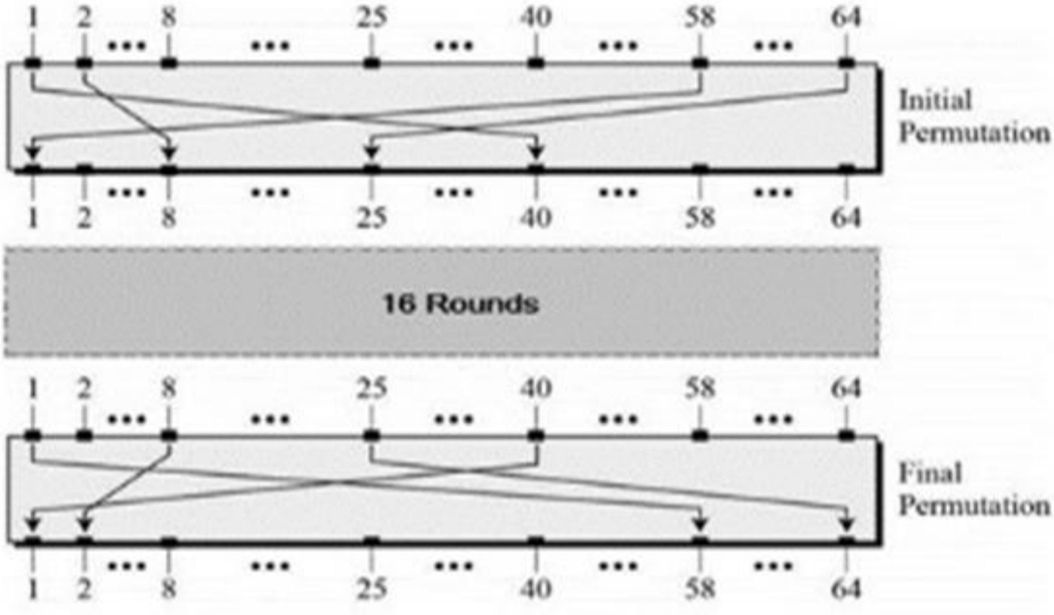

Figure 3: Initial and Final Permutation

D. Round Function

It uses 48-bit key to the right most 32 bits to generate a 32-bit output. During this round function the input is passed through the initial permutation and then the right half data(r0) is rounded with the secrete key and XOR operation is performed with the left half data(l0) then transferred to the next round r1. similarly, all the round function upto round 16 is executed and then perform reverse initial permutation and then the output bits is transferred.

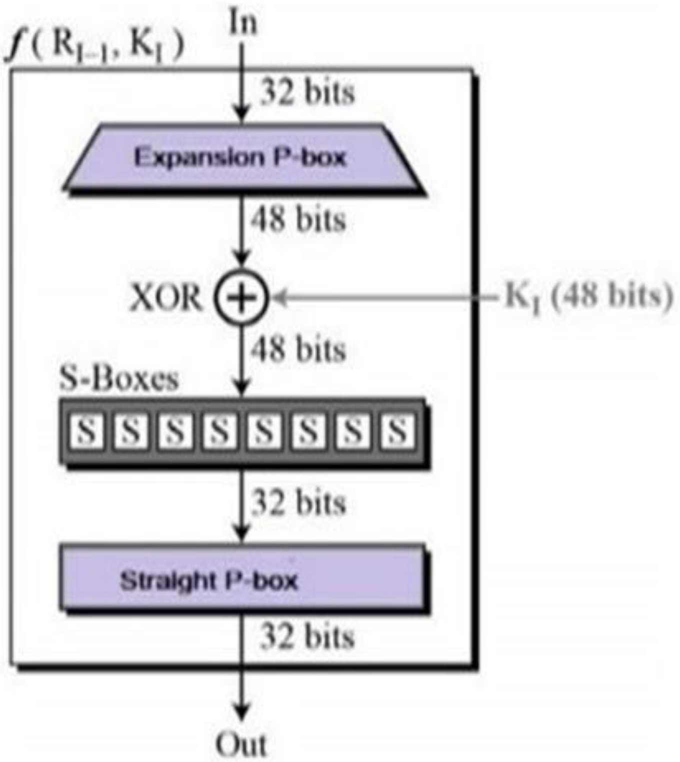

Figure 4: Round Function

- *Expansion Permutation Box* – Due to the usage of an input 32-bit and the round key 48-bit size the right portion of the data is expanded to 48-bits. Permutation logic is shown in the below figure

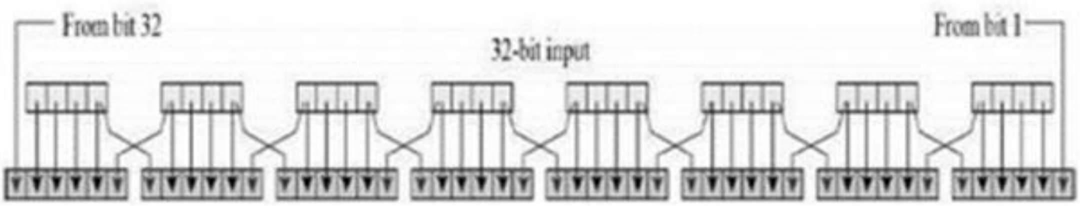

Figure 5: S-Box

The below figure represents a permutation logic as a table

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Figure 6: Expansion Permutation Box

- *XOR (Whitener)* – To follow the expansion permutation DES works on XOR operation on expanded right portion and the round function.
- *Substitution Boxes* − The S-boxes is used to perform confusion. DES utilizes eight S-boxes, each with 6-bit input and a 4-bit output as depicted below

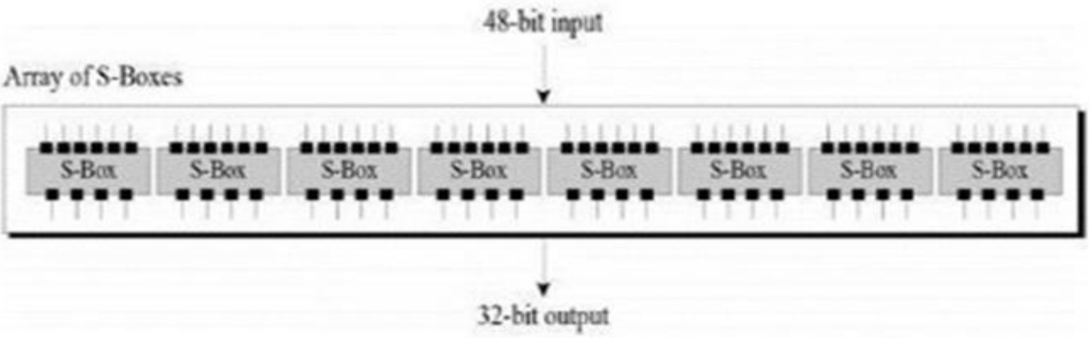

Figure 7: Substitution Box

The S-box rule is shown below

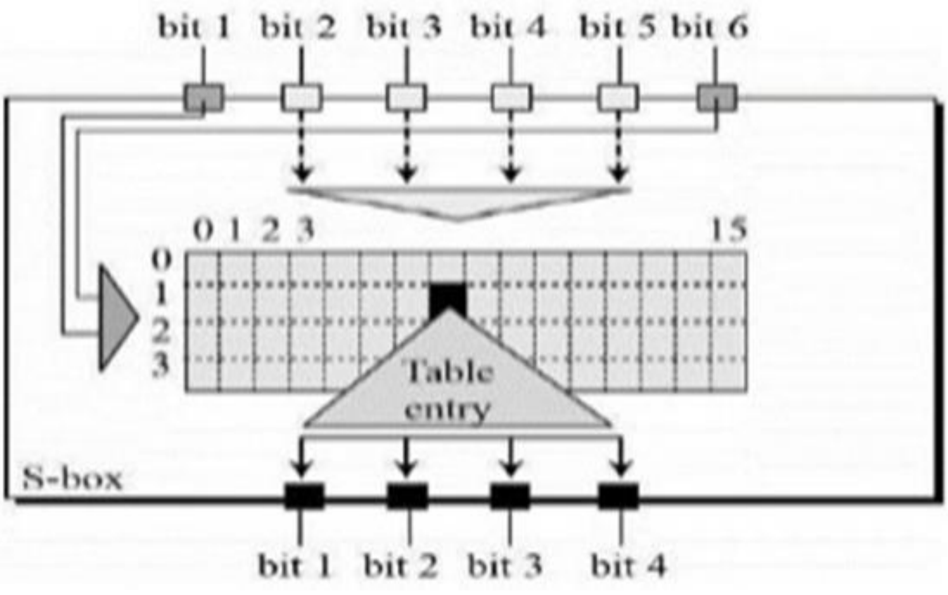

Figure 8: S-box with table

Sum of eight S-box tables is accepted and the output is then merged into a 32- bit section.
Straight Permutation – The below figure depicts the S-box output of 32-bit is passed through the straight permutation.

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

E. Key Generation

A sixteen 48-bit key among 56-bit cipher key is produced using the round-key generator [4]. The process of key generation is shown in the below picture: –

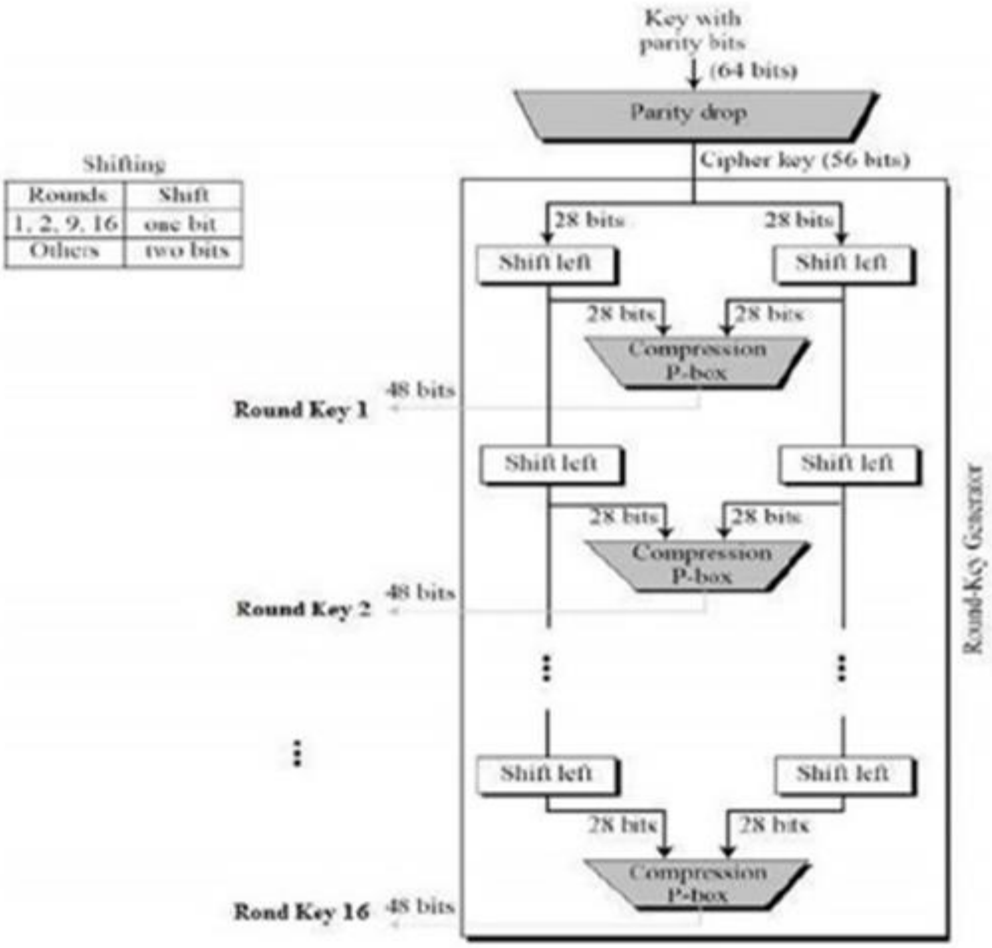

Figure 9: Round Key Generator

F. DES Analysis

The DES analysis can be done based on the two properties such as Avalanche Effect and Completeness.

IV. IMPROVED DATA ENCRYPTION STANDARD USING ZIG ZAG SCAN

A. Introduction

Data encryption Standard has been cracked by many crackers by recent years and can be easily attacked. By introducing improved DES some functions that are hard to decrypt unless you have key for the plain text. Improved DES ensure the features in DES cannot be minimized and can be maintained with high security.

B. Zig-Zag pattern

Zig Zag pattern (ZZ) is a common scanning pattern used in image compression, which is performed on the result of quantization process where the pixel values in a 2-D square matrix is reordered into a 1-D matrix.
Subsequently, a lossless encoding procedure called RLE is applied to the result of Zigzag scan.

Retrieval Number: 100.1/ijitee.F95160512623
DOI: 10.35940/ijitee.F9516.0512623
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

During the scanning, we visit each cell exactly once in some order and bring into being a 1-D matrix. Zigzag pattern scans the 2-D square matrix in a horizontal-diagonal-vertical-diagonal fashion [5].
starting from upper left to lower right.

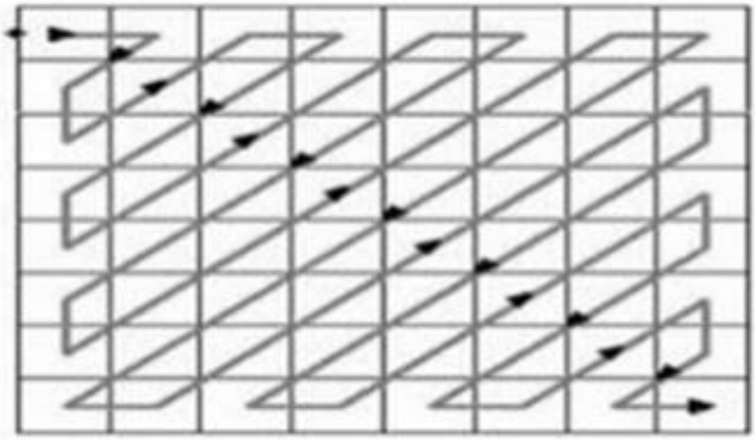

Figure 10: Zigzag Pattern

The algorithm for ZZ is presented below.

Step 0: Initialize row =1 and column =1
Step 1: Move right once by incrementing column by 1
Step 2: Move to the bottom left by incrementing row by 1 and decrementing column
Example of zig-zag scan:

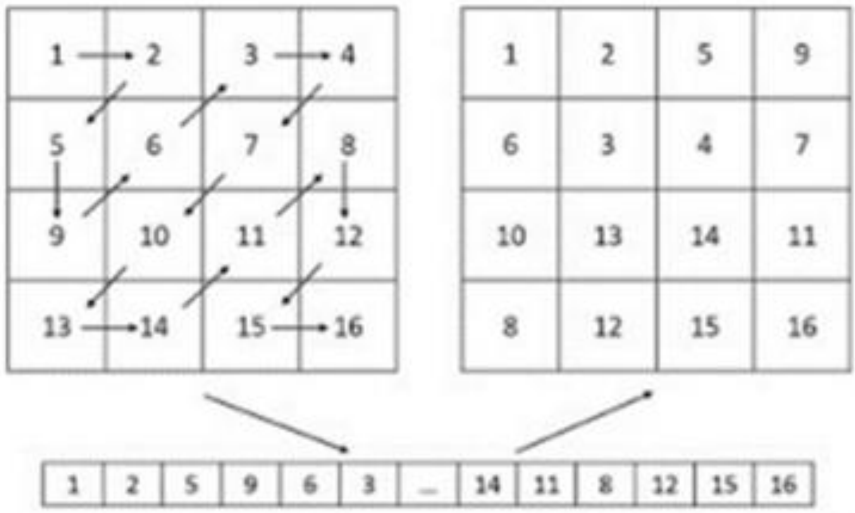

Figure 11: Zigzag Scan

In the given figure one of the methods of zig-zag scan in this method on first given
S=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
For S we have applied a zig-zag scan then S will be converted to
S=1,2,5,9,6,3,4,7,10,13,14,11,8,12,15,16

C. Columnar transposition method

The Columnar Transposition Cipher is an encryption method that exchange the columns of a table. Columnar transposition requires plain text written in rows and then get the cipher text from columns. It rearranges the order of plain text bits. No replacement/substitution.

D. Improved DES Algorithm

The process starts by accepting 64-bit plain text and passed to the initial permutation.

1. The initial permutation rearranges the bits into two portions, named as left-hand portion and right-hand portion.
2. Both the left and right portions go through 16 rounds of the encryption process.
3. In Round function Zig zag scan is performed on SBOX.
4. And then Columnar Transposition is performed on the result after zigzag scan on SBOX.
5. Then the XOR operation is performed in round function
6. ultimately, the left portion and right portion are rejoined, and a final permutation is executed on the recently merged block.
7. A 64-bit cipher text is produced after accomplishing the above steps.

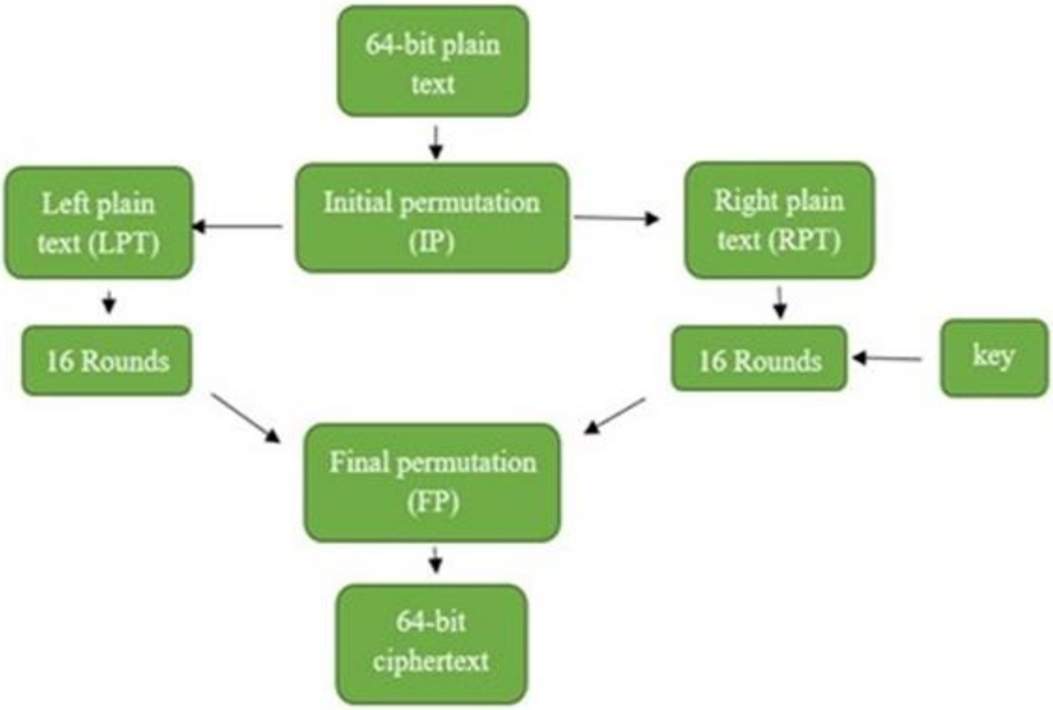

Figure 12: Improved DES

In the above figure there are 16 rounds which introduces some functions called zigzag scan on SBOX and after it will perform columnar transposition in the s-box and then process will continue for 16 rounds.

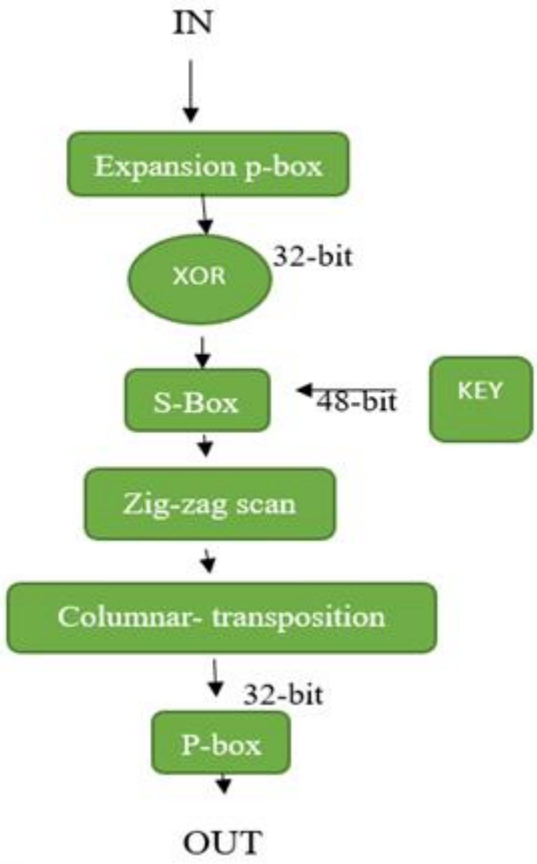

Figure 13: Modified Round function

E. Modified Round Function

From the flowchart it can be observed the functions zig zag and columnar transposition and the output of these function 32 bits are given to the p-box in which these are XORed with the left plain text and then output is produced to the next round.

V. RESULTS

In improved DES it uses Zig Zag Scan for better results and the features like completeness, Avalanche Effect, Encryption Time, and Decryption time is maintained in seconds. Features of Improved DES are Avalanche effect, Completeness.
Encryption time:0.6420354843139648
Decryption time:0.8394386768341064
Examples for Improved DES

Encryption for case1

Table 1. Encryption for case1

```
=== RESTART: C:\Users\chery\AppData\Local\Programs\Python\Python38-32\des2.py ==
-----------Zig Zagged output-----------
14 4 0 4 15 13 1 7 1 15 12 14 4 8 8 2 2 15 14 13 2 11 8 13 6 4 9 2 1 11 1 7 3 10 10 15 6 6 12 12 12 5 11 9 11 7 3 14 5 9 9 3 5 0 7 3 1
0 10 0 5 8 0 6 13 15 1 3 0 13 8 14 4 14 13 8 7 7 11 10 1 6 11 15 10 2 3 4 8 4 3 15 13 14 1 4 2 9 7 12 5 0 2 13 1 8 11 6 12 10 6 7 12 1
2 0 6 9 9 5 10 11 3 0 5 2 5 15 14 9 10 0 13 13 7 9 14 0 6 1 10 4 9 9 13 0 6 3 3 8 4 15 5 6 15 6 9 3 10 0 8 7 1 13 2 11 8 12 7 5 1 4 15
2 14 12 14 3 11 4 12 5 11 2 8 15 10 11 5 14 1 7 2 12 7 13 13 10 8 14 3 11 6 3 15 9 5 0 0 6 0 6 6 12 15 9 10 0 11 10 1 7 3 13 13 8 1 2
4 15 7 8 5 2 1 9 4 3 12 14 5 11 11 12 1 5 10 4 15 14 2 12 7 8 9 4 2 14 2 12 14 4 11 4 1 2 2 11 8 1 12 11 12 7 7 10 4 10 7 11 6 13 13 1
14 7 1 8 2 13 8 5 5 15 0 3 15 15 9 6 15 12 10 5 0 9 13 0 3 6 9 14 9 8 3 10 4 0 6 14 5 3 12 1 10 9 15 10 15 4 14 4 3 15 2 5 2 12 9 2 7
2 12 6 8 9 8 9 5 12 5 3 15 10 0 13 6 7 1 3 4 13 0 11 14 4 14 10 1 7 14 7 0 1 11 5 11 3 13 6 0 11 8 6 8 13 4 11 13 1 0 2 14 11 4 6 11 1
1 7 13 13 8 15 0 4 12 9 8 13 1 3 1 4 7 10 14 10 7 3 12 14 10 3 9 7 5 15 9 5 6 12 8 0 15 5 10 2 0 15 6 1 8 5 14 2 9 6 2 3 12 13 2 1 7 1
5 8 4 13 11 2 1 4 8 1 14 7 6 15 10 9 3 11 1 7 12 4 10 14 4 2 8 13 10 9 12 0 5 3 14 6 6 15 12 10 11 13 9 0 5 0 0 15 14 12 7 9 3 3 5 5 2
8 6 11
 Enter plain text of atleast 16 characters:ABCDEF1234ABCDEF

 Enter key of same size as plain text:123456ABCD123456
Encryption
After inital permutation C618D6E7E7B5E7AD
Round No      left      right      round key
--------------------------------------------------
Round  1    E7B5E7AD   37194EAF   7201C69E3355
Round  2    37194EAF   D1ABCAEB   123E31ED00E7
Round  3    D1ABCAEB   3299955E   CD3C4046EACF
Round  4    3299955E   A3487A26   42E6CC3695DD
Round  5    A3487A26   60DB31DA   58D5028B95E3
Round  6    60DB31DA   F5138C52   60896B4EEF21
Round  7    F5138C52   51A49B8D   A1E0077A4D5C
Round  8    51A49B8D   8A4380A5   210F92C9D19A
Round  9    8A4380A5   8DDD7AAD   6252488DAFF8
Round  10    8DDD7AAD   21B9DF57   08D96439DE51
Round  11    21B9DF57   8B4CC35F   80695B5BC436
Round  12    8B4CC35F   E9B48C60   2567218D6D8C
Round  13    E9B48C60   D952DE09   C31D81A872D5
Round  14    D952DE09   17FA8CEB   59A2D1F3C2A7
Round  15    17FA8CEB   D23EC140   15D48A960F8B
Round  16    FED5D067   D23EC140   842B88353596
Cipher Text :  19E17160F461DFDC
Encryption time:  0.6420354843139648
```

Decryption for case1

Table 2. Decryption for case1

```
Decryption
After inital permutation FED5D067D23EC140
Round No      left      right      round key
--------------------------------------------------
Round  1    D23EC140   17FA8CEB   842B88353596
Round  2    17FA8CEB   D952DE09   15D48A960F8B
Round  3    D952DE09   E9B48C60   59A2D1F3C2A7
Round  4    E9B48C60   8B4CC35F   C31D81A872D5
Round  5    8B4CC35F   21B9DF57   2567218D6D8C
Round  6    21B9DF57   8DDD7AAD   80695B5BC436
Round  7    8DDD7AAD   8A4380A5   08D96439DE51
Round  8    8A4380A5   51A49B8D   6252488DAFF8
Round  9    51A49B8D   F5138C52   210F92C9D19A
Round  10    F5138C52   60DB31DA   A1E0077A4D5C
Round  11    60DB31DA   A3487A26   60896B4EEF21
Round  12    A3487A26   3299955E   58D5028B95E3
Round  13    3299955E   D1ABCAEB   42E6CC3695DD
Round  14    D1ABCAEB   37194EAF   CD3C4046EACF
Round  15    37194EAF   E7B5E7AD   123E31ED00E7
Round  16    C618D6E7   E7B5E7AD   7201C69E3355
Plain Text :  ABCDEF1234ABCDEF
Decryption time  0.8394386768341064
```

Encryption for case2

Table 3: Encryption for case2

```
 Enter plain text of atleast 16 characters:ABCDEF1234ABCDED

 Enter key of same size as plain text:123456ABCD123456
Encryption
After inital permutation C618D6E7E7B5E72D
Round No      left      right      round key
--------------------------------------------
Round  1   E7B5E72D   37296EAE   7201C69E3355
Round  2   37296EAE   50E85AC9   123E31ED00E7
Round  3   50E85AC9   A99142A9   CD3C4046EACF
Round  4   A99142A9   83654694   42E6CC3695DD
Round  5   83654694   E6924E02   58D5028B95E3
Round  6   E6924E02   05A5C6A3   60896B4EEF21
Round  7   05A5C6A3   578228C6   A1E0077A4D5C
Round  8   578228C6   AA8E168B   210F92C9D19A
Round  9   AA8E168B   7AB24539   6252488DAFF8
Round  10   7AB24539   1CE74F85   08D96439DE51
Round  11   1CE74F85   5C5AAE9F   80695B5BC436
Round  12   5C5AAE9F   2EF00EEA   2567218D6D8C
Round  13   2EF00EEA   DF26C105   C31D81A872D5
Round  14   DF26C105   40D35AD4   59A2D1F3C2A7
Round  15   40D35AD4   4DE33D9A   15D48A960F8B
Round  16   2F24D387   4DE33D9A   842B88353596
Cipher Text :  ED67D9CA0E78A427
Encryption time:  0.9885833263397217
```

Decryption for case2

Table 4: Decryption for case2

```
Decryption
After inital permutation 2F24D3874DE33D9A
Round No      left      right      round key
--------------------------------------------
Round  1   4DE33D9A   40D35AD4   842B88353596
Round  2   40D35AD4   DF26C105   15D48A960F8B
Round  3   DF26C105   2EF00EEA   59A2D1F3C2A7
Round  4   2EF00EEA   5C5AAE9F   C31D81A872D5
Round  5   5C5AAE9F   1CE74F85   2567218D6D8C
Round  6   1CE74F85   7AB24539   80695B5BC436
Round  7   7AB24539   AA8E168B   08D96439DE51
Round  8   AA8E168B   578228C6   6252488DAFF8
Round  9   578228C6   05A5C6A3   210F92C9D19A
Round  10   05A5C6A3   E6924E02   A1E0077A4D5C
Round  11   E6924E02   83654694   60896B4EEF21
Round  12   83654694   A99142A9   58D5028B95E3
Round  13   A99142A9   50E85AC9   42E6CC3695DD
Round  14   50E85AC9   37296EAE   CD3C4046EACF
Round  15   37296EAE   E7B5E72D   123E31ED00E7
Round  16   C618D6E7   E7B5E72D   7201C69E3355
Plain Text :  ABCDEF1234ABCDED
Decryption time  0.9185218811035156
```

Avalanche Effect generated for two cases:

Table 5: Avalanche Effect

```
 Avalanche Effect can be observed as:
CASE - 1
 Plain text: ABCDEF1234ABCDEF
 Cipher text: 19E17160F461DFDC
CASE - 2
 Plain text: ABCDEF1234ABCDED
 Cipher text: ED67D9CA0E78A427
>>>
```

Retrieval Number: 100.1/ijitee.F95160512623
DOI: 10.35940/ijitee.F9516.0512623
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

From the results it shows the performance of zigzag scanning approach which enhances the encryption time of the input file with more completeness and better avalanche effect.

VI. CONCLUSION

Now-a-days all the data transfers, business transactions and different kinds of applications are carried out through internet. Providing the security and maintaining the confidentiality will plays a crucial role. Therefore, in this paper the improved DES algorithm is used to provide better security than the traditional DES. The improved DES is designed with a modification in S-box and also uses a zig zag scan method and using the columnar transposition makes it stronger than the DES.

DECLARATION

Funding/Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participation	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/Data Access Statement	Not relevant.
Authors Contribution	S. Hemasri; methodology, S. Hemasri, S.Kiran, and Rajeshkanna Coding, A.Ranichitra; validation, S. Kiran, A.Rajeshkanna, and A. Ranichitra; investigation, S. Kiran and A.Rajeshkanna; resources, S.Hemasri; writing—original draft preparation, S.Hemasri, and S. Kiran; writing—review and editing, S.Hemasri, S. Kiran and A.Ranichitra. All authors have read and agreed to the published version of the manuscript.

REFERENCES

1. Sombir Singh, Sunil K. Maakar, Dr. Sudesh Kumar, "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", Vol3, Issue 6, June 2013, ISSN: 2277 128X.
2. Kaur, N., & Sodhi, S. (2016, October). Data encryption standard algorithm (DES) for secure data transmission. In International Conference on Advances in Emerging Technology (ICAET) (pp. 31-37).
3. Na Su Yi Zhang, Mingue Lithe," Research on Data Encryption standard Based on AES Algorithm in Internet of Things Environment",2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference [ITNEC]2019.
4. Wang Sheng Zhou Jian, "Research on Data Encryption of Network Communication Based on Big Data ",2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering.
5. Khalid Ali Hussein, Sadiq A.m. Mehdi, Salam Ayad Hussein, "Image encryption based on parallel algorithm via zigzag manner with a new chaotic system", Journal of Southwest Jiantong University, vol.54, No.4, Aug 2019 ISSN no.0258-2724. [CrossRef]
6. Pratibha Chaudary, Ritu Gupta, Abhilash Singhc, Pramathesh Majumder, Ayushi Pandey," Joint Image Compression Using a novel column-wise scanning and optimization algorithm", International Conference on Computational Intelligence and Data Science (2019), Procedia computer science 169(2020)244-253. [CrossRef]
7. Li, S., Zhao, L., & Yang, N. (2021). Medical image encryption based on 2d zigzag confusion and dynamic diffusion. Security and Communication Networks, 2021. [CrossRef]
8. Elkandoz, M. T., Alexan, W., & Hussein, H. H. (2019, April). Double-layer image security scheme with aggregated mathematical sequences. In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-7). IEEE. [CrossRef]
9. Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, Wojcicch Mazurczak, "Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario", IEEE Transactions on Network and Service Management, Vol.17 no.1, mar 2020. [CrossRef]
10. Shanshan Li, Li Zhao and Na Yang, "Medical Image Encryption Based on 2D ZigZag Confusion and Dynamic Diffusion", Hindwai Security and Communication Networks, Vol.20, article ID:6624809.
11. Harshali D. Zodpe, Prakash Wani, rakesh R. Mehta: Design and Implementation of algorithm for DES Cryptanalysis", Hybrid Intelligent Systems, 2012 12th International Conference.
12. Mohit Agarwal," Ensuring Data Security in Databases using Format Preserving Encryption", 978-1-5386-1719-9/18$31.00 2018 IEEE.

AUTHORS PROFILE

Singareddy Hemasri received the B.Tech. and M.Tech degrees in computer science and engineering from JNTUA Anantapur, India, in 2011 and 2013, respectively. She is currently pursuing the Ph.D. degree with the Department of Computer Science, Madurai Kamraj University, Madurai. Her current research interests include wireless sensor networks and Cryptography.

Dr. S.Kiran is associate Professor in the department of Computer Science and Engineering at Yogivemana University, Proddatur. He acquired M.Tech Degree from Nagarjuna University, Guntur. He completed Ph.D in computer Science in Computer Science from S. K. University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals. His research areas are image processing, Cryptography and Network Security, Software Engineering and Data mining and Data ware house.

Dr. A.Ranichitra received the MCA degree from P.S.G.R Krishnammai College for Women Coimbatore, in 1999, the M.Phil, Mother Teresa Women's University, Kadaikanal, India, in 2004, and the Ph.D. degree Manonmaniam Sundaranar University, Tirunelveli, India, in 2016.She is currently an Assistant Professor with the Department of Computer Science, S.Ramasamy Naidu Memorial College, Sattur. Shee has contributed several publications in reputed international journals and conference. Her research interests include VANET, Machine Learning, Image Processing, Data Mining.

Dr. A.Rajesh Kanna received the M.sc degree from Alagappa University, Karaikudi, in 1998, the M.Phil. Manonmaniam Sundaranar University, Tirunelveli, India, in 2004, and the Ph.D. degree from the S.Ramasamy Naidu Memorial College, Sattur, Madurai, India, in 2021. He is currently an Assistant Professor with the Department of Computer Science, S.Ramasamy Naidu Memorial College, Sattur. He has contributed several publications in reputed international journals and conference. His research interests include Data Mining, Computer Networks.

Retrieval Number: 100.1/ijitee.F95160512623
DOI: 10.35940/ijitee.F9516.0512623
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)