International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

Moulded RSA and DES (MRDES) Algorithm for Data Security

S. Jenifa Sabeena[a]*, Dr. S. Antelin Vijila[b]
[a]*Research Scholar,
Manonmaniam Sundaranar University,
Tirunelveli, India
e-mail: jenifamsu@gmail.com
[b]Assistant Professor,
Manonmaniam Sundaranar University,
Tirunelveli, India
e-mail: antelinvijila@gmail.com

Abstract—In the recent days transmission of large amount of data through online is very prominent. Security is necessary while transmitting large amount of data. Since the data may belost or hacked at some point of transmission. Normally there are three important factors interms of security. They are key generation, encryption and decryption. There are two types of crypto system namely symmetric cryptosystem and asymmetric cryptosystem. There are many publicly available cryptosystems. It may lead the intruders to view the original message sent by the sender using all the possible keys. In order to provide secure transmission of data, a novel encryption algorithm is proposed by analyzing all the existing algorithms. The existing Rivest–Shamir–Adleman (RSA) and Data encryption standard (DES) algorithm are moulded together rto produce the proposed MRDES encryption algorithm. The performance of the proposed Moulded RSA and DES is higher than the existing encryption algorithms and provides higher data security.

Keywords-MRDES encryption, Rivest–Shamir–Adleman (RSA) Dataencryption standard(DES), decryption and data security.

I. INTRODUCTION

Now a day's data plays a vital role in human lives. Data is very crucial as it needs protection from the intruders. Security is done to protect the data from unauthorized users so that data cannot be modified or changed by them [1-2]. The act of protecting data from unauthorized access is called confidentiality. Data must be secured in a way that it should only authorized users can access it. Normally the data gathered by any individual or companies are stored as records. The confidentiality of the stored data became progressed via lowering the un authorization of user's data and proscribing the users by records change [3-4]. Cryptography is the method of protecting data from the unauthorized person. The cipher text and plain text are the basic elements in cryptography [5]. The plain text is the original form of data which must be protected during the transmission. The cipher text is the unreadable form of the plaintext after encryption. In the process of encryption, plain text is converted into cipher text and cipher text is converted into plain text in decryption [6]. The key is a piece of data and must be kept secret as the algorithm is publicly available. The encryption key is the value that is used by the sender and decryption key is used by the receiver [7]. The modern cryptography is classified into two types they are symmetric and asymmetric key algorithm. The symmetric cipher uses same key for the encryption and decryption process. This is known as secret key cryptography. AES, Diffie Hellman, DES and Blowfish are the symmetric key algorithms [8-10]. DES was developed in the year 1970 and it is one of the symmetric block ciphers. DES works on feistel cipher structure. Feistel proposed a scheme to produce a block cipher using the permutation and substitution process. The overall interchange of the values of the two half of the data is called permutation [11]. This form of the structure is called as the Substitution and Permutation Network (SPN).Comparing to asymmetric key algorithm the utilization of resources is low and the execution is faster [12].

In a symmetric key cryptography the encryption and decryption process are performed using different keys. This is known as the public key cryptography and the working principle is opposite to symmetric key algorithm [13-14]. Two different keys namely the public key and private key is needed for asymmetric key algorithm. For encryption public key is used and for the decryption process the private key is used. Public key can be given to anyone and private key is kept private. The cipher text is larger or in the same size as the key [15-17]. The asymmetric key algorithm provides authenticity and confidentiality to the user. The resource utilization is higher, when compared to symmetric key algorithm as there sources are involved in exchanging secret keys securely. From the comparison of the cryptographic algorithms, it is concluded that DES and RSA algorithm has high efficiency compared to other algorithms [18].

The contribution of this work is as follows:

- In cryptographic algorithms, DES is scalable as they have the feistel structure and RSA algorithm has high power consumption as the computation time.
- RSA algorithm provides high security for the user data. RS Algorithm is tunableasitis a symmetric in nature.
- To achieve high data security and lower power consumption, the RSA and DES algorithms are moulded to produce a proposed Moulded RSA and DES (MRDES)algorithm.
- The efficacy of the proposed method is proved by the analysis of throughput, energy consumption, encryption and decryption time analysis with RSA and DES approaches.

The remaining part of this paper is organized as follows; the existing techniques are reviewed in the relatedworkSection2. The proposed methodology and the process of proposed MRDES technique is explained in Section 3. The experimental analysis of the proposed technique is discussed in Section 4. Finally, the proposed methodology is concluded in Section5.

II. RELATED WORKS

Data security is an important concern in storing data in the clouds. Cryptographic techniques are among the most significant method stooffer data protection in the cloud. Bermanietal.,[19] presented a data protection approach based on hy brid cryptographic algorithm. The hybrid algorithm is the combination of the advanced encryption standard (AES), Message-Digest algorithm and Blowfish. Therefore, this method offers speed and robust data encryption. To compromise the critical security, a new hybrid steganography and cryptographic scheme was proposed by Baagyere et al [20]. In order to encrypt the text within the images, the genetic algorithm operator was used.

Cloud sources have trouble guaranteeing file safety because security is a huge issue in data handling, as it can access, misuse and erase the original data form. To overcome the security problem and accomplish the CIA (Confidentiality, Integrity, Availability) property the cryptography is used. The outdated asymmetric and symmetric methods have some limitations. To overcome the limitations, Chinnasamy et al., [21] had proposed a hybrid system to achieve high confidentiality and data security. ECC (Elliptic Curve Cryptography) and Blow fish algorithm is hybridized to create a new algorithm. This research examines various security methods and complications from a programming and equipment perspective for protecting data in the cloud. It also focuses on improving cloud data security insurance. Sreedhar eta l[22] proposed an experimental investigation of the current research work on data security and security protection strategies used in a distributed computing.

Al- Hamami and Abdallah [23] proposed a third prime number based on the public and private keys and proposed an enhanced RSA algorithm. In the enhanced RSA algorithm, the factoring variable is enhanced. Priyanka et al., [24] proposed an RSA Digital Signature Algorithm for solving the factorization complexity. The proposed RSADSA is susceptible for factorizing the prime numberd and exponente. In Anjula and Navpreet [25],various cryptographic algorithms were studied and analyzed to find best encryption algorithm. Using a unique ID, the blowfish algorithm performed better in terms of providing high throughput and low power consumption.

Reema [26] introduced a novel algorithm for encryption to offer efficient security.Various encryption algorithms were studied and described in detail. For data encryption huffmann coding was used. Sushil [27]was introduced a novel cubical method-based encryption technique. It is based on the principle of block cipher. The proposed algorithm works with cubes. Each cell has two binary inputs. The EES (Escrowed Encryption Standard) algorithm performs better with bit transformations, S-BOX, XOR and AND operation.

An asymmetric cryptography method called modified RSA algorithm was introduced by Das et al., [28] to protection against the malicious attacks. The proposed scheme reduces the complexity of the RSA algorithm and introduce a new method for determining the value of the public and private keys. In addition, cipher text and plaintext are being discovered by new formula. However, there are still some challenges in the field of RSA algorithm research. To reduce the time, it takes to send data over the Internet, Wahab et al [29] proposed a hybrid data compression algorithm. It enhances the input data to be encrypted by the RSA encryption system to increase the level of protection and it isused to implement loss and lossless abbreviated steganography approaches. This technique can be used to reduce the size of each transferred data or to take up less space on various storage media, which helps in faster transfer when using slow internet. Therefore, the RSA and DES algorithms are designed to implement aninnovative method to improve data security and performance.

III. PROPOSED METHODOLOGY

The proposed architecture for encryption process is derived from RSA and DES. There are two phases in the proposed work. In the first phase, the job card details from the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

vehicle service center are collected. Then entire service details of the vehicle such as date, reason, cost etc., are stored in the data base.

The second phase is to provide data security. Here better security is provided for successful authentication for the information stored in the database. Encryption and decryption are carried out with the help of MRDES algorithm. The RSA and DES algorithm are moulded and named as MRDES.

A. Input Data

In the first phase, all the information regarding the vehicle is collected when the car enters the servicing area of the car service center. Then these details will be stored in the database. T he input data is intext format containing various fields like vehicle number, cost of car service, date, time etc. The real time dataset is used for evaluation purpose. Figure 1shows the sample input data.

	A	B	C	D	E	F	G	H	I	J
1	Dept	JobDate	jobno	Vehicleid	UnitNo	Reason	Notes	CostParts	CostLabor	CostTotal
2	1020	1/14/2021	14073	118743	14	04 DRIVER S REPORT	PM SERVICE CHECK TURN SIGNAL CLUNKING NOISE \	493.85	0	493.85
3	1020	1/15/2021	14232	230973	13	08 PM SERVICE	SERVICEROB EXT 5604	38.87	0	38.87
4	2111	1/15/2021	14006	1243	116	04 DRIVER S REPORT	NEED 4 PLOW PINS	45	0	45
5	2111	1/15/2021	14140	B39109	178	04 DRIVER S REPORT	INSTALL SPINNER ASSY	175	0	175
6	1020	1/15/2021	14163	574950	215	13 SNOW BREAKDOW	DONT START	140	0	140
7	1020	1/15/2021	14169	A00413	283	04 DRIVER S REPORT	DOG BONE PIN BROKEN	358.58	0	358.58
8	2111	1/15/2021	14000	766153	248	08 PM SERVICE	NEED SERVICE CHECK BRAKES	2139.35	0	2139.35
9	2111	1/15/2021	14155	525670	232	04 DRIVER S REPORT	HYD CAP CHECK ENGINE LIGHT ON	163.47	0	163.47
10	1020	1/15/2021	14157	621909	213	40 NEGLIGENCE	TARP VALVE STICKINGRIGHT SIDE MIRROR BRACKET E	241.33	0	241.33
11	1020	1/15/2021	14164	1226	117	13 SNOW BREAKDOW	HANDLES IN CAB LOOSE	233.42	0	233.42
12	2111	1/15/2021	14165	525999	114	04 DRIVER S REPORT	NO PLOW LIGHTS	11.91	0	11.91
13	2111	1/15/2021	14172	B34632	276	10 ROADCALL	WILL NOT START	1.79	0	1.79
14	1020	1/15/2021	14174	1469	122	10 ROADCALL	WILL NOT START	98.08	0	98.08
15	1020	1/15/2021	14175	68932	147	10 ROADCALL	WILL NOT START	397.87	0	397.87
16	2111	1/15/2021	14176	68933	148	10 ROADCALL	WILL NOT START	358.58	0	358.58
17	2111	1/15/2021	14177	621907	208	10 ROADCALL	WILL NOT START	2139.35	0	2139.35
18	2111	1/15/2021	14181	337657	218	04 DRIVER S REPORT	CONVEORY NOT WORKING	163.47	0	163.47
19	1020	1/15/2021	14182	D1920	164	10 ROADCALL	DONT START	241.33	0	241.33
20	1020	1/15/2021	14183	525998	217	10 ROADCALL	DONT START	233.42	0	233.42
21	2111	1/15/2021	14184	526000	225	10 ROADCALL	DONT START	11.91	0	11.91

Figure1. Sample Input data

B. PROPOSED MRDES ALGORITHM

The proposed MRDES algorithm is one of the symmetric encryption algorithms. It is a block cipher (plain text and cipher text is of same size). MRDES is created from RSA and DES algorithms, since DES have good encryption and low power consumption while RSA provides a good key generation process. The key generation process is performed using RSA algorithm and the encryption is carried out using the DES algorithm.

Figure 2 shows the overall working of the MRDES algorithm. At first the job card details are given as input for the plain text, and then the initial permutation is performed. When the data enters into the round function the key generation process is performed. Then the 16round encryption process is done. At the end of the 16 round encryptions process the final permutation is done and the cipher text is generated.

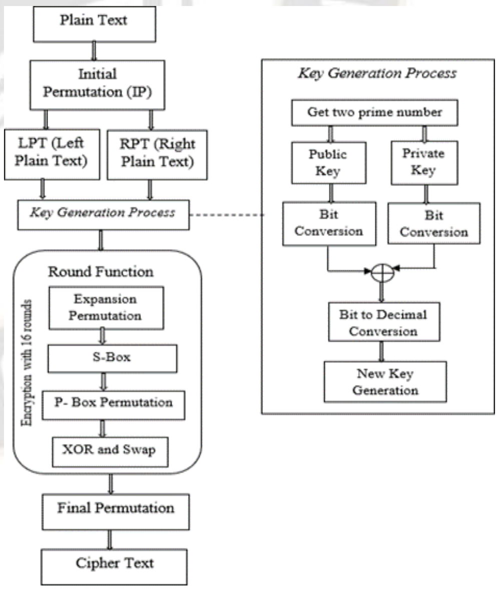

Figure 2. Proposed MRDES Architecture

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

Algorithm: Moulded RSA and DES

Input: i data
Step 1: Starts with 64-bit plain text block and given to an IP function
Step 2: IP is accomplished on the plain text
Step 3: IP creates permuted blocks of LPT and RPT
Step 4: Key generation is performed using **Function Key Gen()**
Step 5: LPT and RPT goes through 16 rounds of the encryption
Step 6: DES encryption process
Step 7: The LPT and RPT are re-joined, and FP is accomplished on the new block
Step 8: Obtain result

Function Key Gen()
Step 1: Chosen two prime number p and q, where $p \neq q$
Step 2: Compute$n = p * q$, where n= block size
Step 3: Compute$\emptyset(n) = (p-1)*(q-1)$
Step 4: Select e which is relatively prime to $\emptyset(n)$
Step 5: Calculate $d = e - 1 \; mod \; \emptyset(n)$
Step 6: $Public\ key = \{e, n\}, private\ key = \{d, n\}$
Step 7: Converts public and private key to bit using bit conversion process
Step 8: Converted bit is XOR ed and random permutation is performed
Step 9: New bit is generated and decimal conversion is performed
Step 10: New input key is generated (DES input key)
End Function

There are5 steps in MRDES algorithm and the steps in the algorithm are as follows,

- Initial Permutation
- Key Generation process
- 16roundencryption process
- Final permutation
- MRDES decryption

1) Initial Permutation (IP)

Initial Permutation is a bitwise permutation and performed only once. In initial permutation the bit sequence is changed as per the Figure 3 that is shown below and theresult of the bit swap is shown in the Figure 4 (a, b).

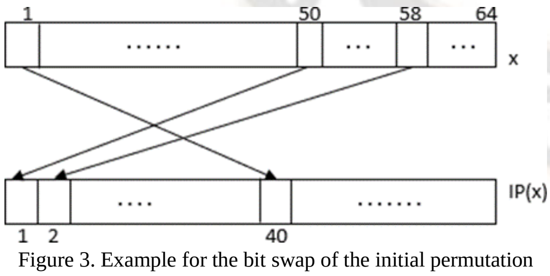

Figure 3. Example for the bit swap of the initial permutation

Before Permutation							
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Figure 4 (a). Before Permutation

IP							
50	58	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	24	16	6
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Figure 4 (b). Initial Permutation

The IP table shows the mapping of bit 58 with output position 1, mapping of bit 50with 2nd output position. The initial permutation is completely carried out on the 64-bit plaintext block.

2) Key Generation

The key generation is carried out using the RSA algorithm. In the first step, two prime numbers, p and q, are selected, and by multiplying p and q values, n is calculated. Using the formula $\emptyset(n) = (p-1)*(q-1)$, the value of $\emptyset(n)$ is determined. Next the value of e is selected and it must be relatively prime to$\emptyset(n)$. The value of $d$is then calculate using the formula d=$e - 1$ mod $\emptyset(n)$. The public key is given as $\{e, n\}$, while the private key is given as $\{d, n\}$. After that, the public and private keys are converted to bits using the bit conversion process, and the bits are then XO Red and a random permutation is performed. By generating a new bit and performing a decimal conversion, the new input key can be generated, which is given as an input key for DES.

3) Sixteen Round of Encryption

The encryption follows16round processes, the working is based on the feistal structure. Then the plaintext is divided into LPT and RPT in the size of 32 bits. It is the input of feistel network and it contains 16 rounds. The RPT right half is applied to function f and the output is XORed with the left half LPT Finally, the two halves are swapped and the same process is repeated in the further rounds. After 16 rounds, the $L16$ and $R16$ are exchanged once again in the final permutation of MRDES. Decryption is bottom-up process of encryption.

The 16 Round of Encryption contains the following steps

- Key Transformation
- Expansion Permutation
- S-Box Substitution
- P-Box Permutation
- XOR and Swap

Key Transformation

The 64-bit original key passes through the key discarding process where the eight bit of the original key is discarded and producing 56-bit key. The 56-bit key then passes through the key bit shifting process. The key is divided into two equal halves of 28-bit each and a circular left shift is performed on each half. The shifting of bit positions depends on the round; for round number 1,2,9,16 the left shift is done by one position and for all other rounds the left shift is done by two positions. Once the key bit shifting process is complete, the 56-bit key goes through the compression permutation. The 56-bit key is compressed to 48-bit key by

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

dropping the bits in position 9,18,22,25,35,38,43,54.

Expansion Permutation

In expansion permutation the 32-bit RPT is expanded to 48-bit. It is done by dividing 32-bit RPT into 8 blocks each of 4-bits. The 4-bit block is prolonged to 6 bit and produce 48-bit output. The expansion permutation is illustrated in Figure 5. The 48-bit RPT is XORed (denoted by ⊕)with48-bit key and output is applied into S-Box.

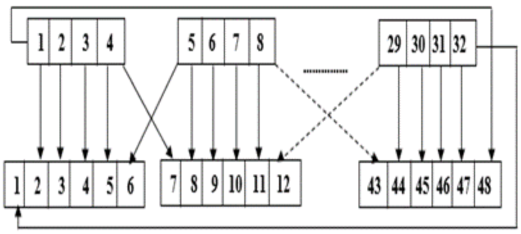

Figure 5. Expansion permutation

Substitution

The XORed result from expansion permutation step is given as input to S-Box substitution. Figure 6 shows the S-Box substitution

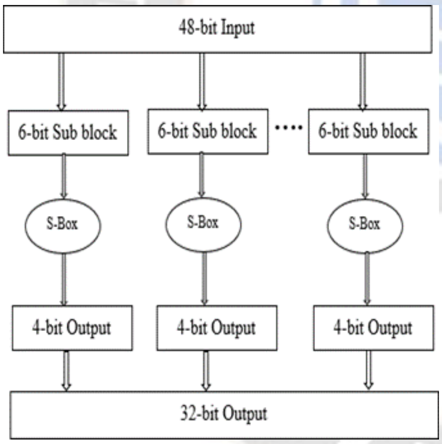

Figure 6. Process of S-Box substitution

The 48-bit input is allocated into eight 6-bit sub blocks. The S-box is referred as the lookup table where the input of 6-bit is mapped to a 4-bit output. The resultant 32-bit output of S-Box substitution is given as the input to the P-Box permutation.

P-BOX PERMUTATION

In this step the incoming 32-bit is permuted to produce a 32-bit output.Figure7showsan example, result of the P-Box permutation where the 16^{th}-bit of the S-Box take the initial position in the P-Box permutation result.

P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Figure 7. P-Box Permutation

XOR AND SWAP

Figure 8 shows the first round of the encryption process. As shown in Figure 8, the32-bit LPT is XORed with the 32-bit output from the P-Box and yields 32-bit RPT. The 32-bit RPT is swapped to 32-bit LPT. After completing the first round the remaining rounds are carried out.

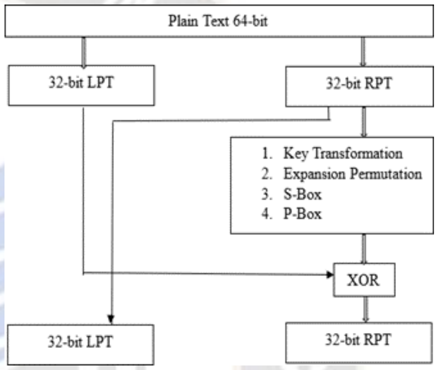

Figure 8. First Round of Encryption

4) Sixteen Round of Encryption

After completing the encryption with 16 rounds final permutation is carried out. The final permutation is the opposite of initial permutation. It is a bit wise permutation and performed only once.Figure9 shows the bit swap operation that will be held in final permutation. The resultant output for final permutation is the 64-bit Cipher Text.

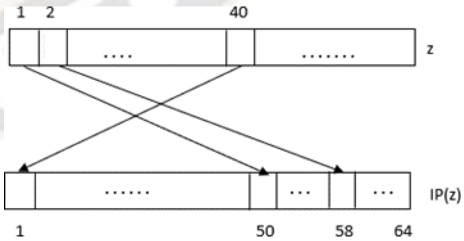

Figure 9. Example for the bit swap of the final permutation

IV. EXPERIMENTAL ANALYSIS

The proposed algorithm is implemented in Python. It has been tested on the system configuration Intel(R)Pentium(R) CPU, 4GBRAM, 64bit Operating System,x64- based processor. The input plain text contains the records of vehicle job card details. Encryption is done for the various key values such as 8, 16, 24, 32, 64, 192, 256, 448, and 512. The input

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

data is encrypted and the cipher text is found, then the performance is measured using the metrices such as encryption time, encryption throughput, energy consumption and computational time analysis. Also, the cipher text is decrypted and the performances of these algorithms are measured using the above said metrices.

The big key length can be utilized for encryption and decryption process to increase the security strength. So, in this work a 512-bit key length is used in the encryption process, which is quite good to protect against attacks. To show the efficiency of the MRDES approach, the introduced method is compared with conventional techniques of DES and RSA. For this, existing DES and RSA method is considered to compare the result with the proposed encryption method MRDES. The comparative result of encryption method is analyzed based on the throughput, energy consumption, execution time of encryption and decryption for different key size.

A. Throughput Analysis

The throughput is used to measure the data transfer rate. The encryption throughput is calculated using total number of data blocks successfully transferred and the time taken for encryption measured in terms of seconds. The decryption throughput is calculated using the total number of data blocks (cipher text in bytes) successfully transferred divided by the time taken (decryption time in seconds). Table 1 shows the results achieved using the algorithms DES, RSA and MRDES. The performance is measured for different key sizes of encryption and decryption throughput.

From the experimental results it is evident that the proposed MRDES offers the best pocket delivery rate. From Table 1, it is clear that if the total number of key size increases, the throughput is also increased. In case of encryption throughput, MRDES achieves 135.82 sec, 156.51 sec, 174.91 sec and 182.2 sec for the key sizes 8, 16, 24 and 32respectively.Indecryption for the key sizes 8, 16, 24 and 32, MRDES achieves the through put rate of 118.16 sec,144.17 sec, 153.83 secand171.64 sec respectively.

TABLE I. ENCRYPTION AND DECRYPTION THROUGHPUT

Algorithm	Input Data (No.of Records)	Key size	Encryption Throughput in sec	Decryption Throughput in sec
DES	170	8	38.72	32.3
		16	49.1	43.81
		24	53.41	50.29
		32	62.35	54.65
RSA	170	8	92.22	89.37
		16	105.54	97.24
		24	118.97	102.37
		32	124.15	119.13
MRDES	170	8	135.82	118.16
		16	156.51	144.17
		24	174.91	153.83
		32	182.2	171.64

The throughput analysis shows that MRDES algorithm outperforms DES and RSA algorithms and provides better encryption and decryption throughput.

B. Encryption And Decryption Time Analysis

Based on different key sizes, the total time analysis is performed for the proposed MRDES approach for the text size 19970. Figure 10 (a, b) shows the line chart for the time consumption analysis of encryption and decryption process. From the observation, when the input key size is increased the total time for encryption is also increased. In case of encryption time, MRDES achieves 0.62 ms, 0.71 ms, 0.75 ms and 0.83 ms for the key sizes of 8, 16, 24 and 32 respectively. In case decryption time, MRDES achieves 0.66 ms, 0.73 ms, 0.78 ms and 0.84 ms for the key sizes 8, 16, 24 and 32respectively.

TABLE II. TOTAL ENCRYPTION AND DECRYPTION TIME

Algorithm	Input Data (No.of Records)	Text Size	Key size in bits	Encryption time (ms)	Decryption time (ms)
DES	170	19970	8	0.68	0.72
			16	0.74	0.76
			24	0.79	0.81
			32	0.86	0.89
RSA	170	19970	8	0.65	0.68
			16	0.72	0.75
			24	0.77	0.79
			32	0.85	0.86
MRDES	170	19970	8	0.62	0.66
			16	0.71	0.73
			24	0.75	0.78
			32	0.83	0.84

In Table 2, the proposed MRDES method takes less time for the encryption and decryption process compared to the DES and RSA method. From the comparative results, it has been demonstrated that the proposed work restores encryption and decryption time. Therefore, the proposed method has low time complexity than the compared methods

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

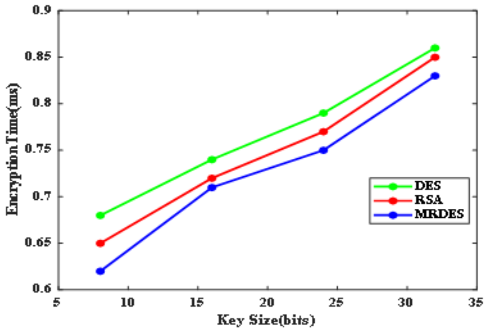

Figure 10 (a). Encryption Time Analysis

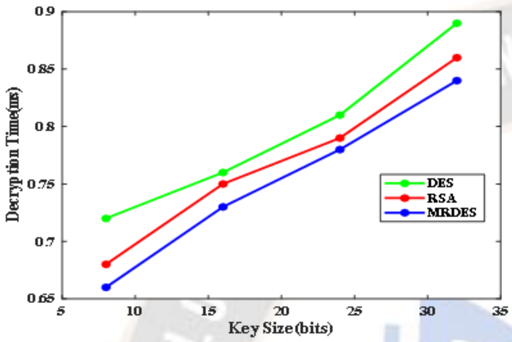

Figure 10 (b). Decryption Time Analysis

C. Analysis of Energy Consumption

The energy consumed for the encryption process is calculated using the equation (1). It is expressed as the number of clock cycle needed for the completion of encryption and average current haggard for each of the CPU clock cycle.

Energy consumption,

$$E=V_{CC}*I*N*r \quad (1)$$

Where, V_{cc} = supply voltage of the system, I = average current, N = number of clock cycles, r = clock period $T=N/processorspeed$ (seconds).

For 170 input data records, the energy consumed for both encryption and decryption are made and tabulated in Table 3.

TABLE III. ENERGY CONSUMPTION

Algorithm	Input Data (No.of Records)	File size KB	Key size	Energy Consumption in Joules
DES	170	5	8	10.39
		10	16	11.56
		15	24	11.56
		20	32	22.14
RSA	170	5	8	9.13
		10	16	10.51
		15	24	10.56
		20	32	13.58
MRDES	170	5	8	7.15
		10	16	7.22
		15	24	8.54
		20	32	9.27

Energy consumption for the three algorithms AES, RSA and MRDES are calculated for different file size and key size. The fact is energy consumption is directly proportional to the time taken for encryption and decryption. Energy consumption for encryption and decryption in MRDES algorithm is 7.15mJ, 7.22mJ, 8.54mJ and 9.27mJ for the file sizes 8,16,24 and 32. The above comparison shows that the proposed MRDES algorithm has better energy consumption when compared to other algorithms.

D. Analysis of MRDES

In the previous analysis section, it is proved that MRDES tops the algorithms DES and RSA in all aspects. This section aims to check the strength of MRDES for the higher values of data size and key size. The performance of MRDES is measured for the increased number of records i.e., 1000 and for the key sizes 64,192,256,448,512 and tabulated in Table 4

TABLE IV. PROPOSED MRDES ALGORITHM PERFORMANCE

Input Data	Text Size	Key size	Execution Time (ms)	Encryption Through put (sec)	Decryption Through put (sec)	Energy in Joules
1000	109229	64	1.5935	219.54	207.12	9.96
		192	1.6094	230.71	226.46	9.96
		256	1.6228	281.83	272.72	10.08
		448	1.6405	327.40	315.71	10.54
		512	2.0157	356.88	349.43	14.84

As of right now, encryption algorithms only use short key lengths, however the algorithm is strengthened by setting the key length at the highest point and computing the values. According to this analysis, the proposed algorithm is efficient even when the key length is long. Based on these results, it is concluded that an increase in key size improves the performance of the MRDES algorithm and a key size of 512 bits will be used for future analysis.

The input data is altered from the lower range to the higher range, i.e., from 200 records to 1000 records, in order to test the proposed algorithm. In Table 5, MRDES' performance is spotted, even when the number of records is increased; it still works efficiently.

TABLE V. PROPOSED MRDES ALGORITHM PERFORMANCE FOR DIFFERENT INPUT DATA

Input Data	Text Size	Key size	Execution Time (ms)	Encryption Throughpu t (sec)	Decryption Throughpu t (sec)	Energy in Joules
200	21070	**512**	1.56	**358.23**	**327.51**	9.76623
400	42197		1.57	**372.37**	**346.44**	9.7666
600	63241		1.57	**426.16**	**421.38**	9.9605
800	84346		1.59	**480.87**	**466.69**	9.9611
1000	109229		1.68	**501.19**	**497.84**	11.1330

ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6140
***Article Received**: 24 December 2022 **Revised**: 20 January 2023 **Accepted**: 22 January 2023*

A fitness function measures how close a given solution is to the optimum solution of a problem. The fitness value is calculated based on equation (2),

$$\text{Fitness value} = 1/|x+y+z-t| \quad (2)$$

X and Y denote encryption and decryption throughput, z represents energy consumption, and t represents execution time.

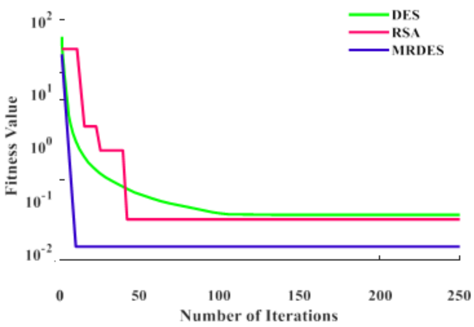

Figure 11. Fitness evaluation

Figure 13 shows the fitness evaluation of proposed and existing methods of DES and RSA. The fitness comparison is made for fitness value versus total number of iterations. From the above performance also the MRDES algorithm proves the better performance than the other algorithms.

V. CONCLUSION

As internet usage has become part of our daily lives, growing explosively during the last several decades, data security has become one of the biggest concerns. User expectations of their personal data should be very safe for transmission over the open network, and it can be accomplished only by a very powerful algorithm. Keeping the data secure ensures that only the intended recipient is able to access it, and it prevents any modification or alteration. Numerous algorithms and methods have been developed so as to achieve this level of security. The security of any type of algorithm depends on the secrecy of the key and encryption method. For providing security to data two algorithms RSA and DES are moulded together to produce MRDES. The proposed MRDES method proves the better performance by the comparative analysis of existing techniques of RSA and DES. The analysis is performed in terms of throughput, energy consumption, fitness evaluation, time computation of encryption and decryption process. When increase the input data, the proposed system is also providing better performance. Hence, it is proved that the MRDES algorithm provides better security to data by setting high key value.

ACKNOWLEDGMENTS

I confirm that all authors listed on the title page have contributed significantly to the work, have read the manuscript, attest to the validity and legitimacy of the data and its interpretation, and agree to its submission.

REFERENCES

[1] R.A Popa, and Zeldovich, "Multi-Key Searchable Encryption", IACR Cryptologye Print Archive, pp.508, 2013.

[2] C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou, and R.H. Deng, "Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, vol.25, no.2, pp.468-477, 2014.

[3] M.S.P. Jadhav, and B.R. walkar, "Efficient Cloud Computing with Secure Data Storage using AES", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 6, pp. 377-381, 2015.

[4] P.V. Nithyabharathi, T. Kowsalya, and V. Baskar, "To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES", International Journal of Science, Engineering and Technology Research (IJSETR), vol. 3, no. 2, pp.341-345, 2014.

[5] Ghavghave, S. Rashmi, and Deepali M. Khatwar, "Architecture for Data Security in Multi-Cloudusing AES-256 Encryption Algorithm", International Journal on Recent and Innovation Trends in Computing and Communication, PP. 2321-8169, May 2015.

[6] D.W. Chadwick, and K. Fatema, "A Privacy Preserving Authorization System for the Cloud", J.Computing System Science, vol. 78, no. 5, pp.1359-1373, 2012.

[7] S. Hou, T.Uehara, S.M.Yiu, L.C.K.Huiand K.P.Chow, "Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers", Proceeding of 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2011, pp: 378-383, DOI: http://dx.doi.org/10.1109/IIHMSP.2011.28

[8] S. Pearson Y. Shen and M. Mowbray, "A privacy manager for cloud computing", In:Jaatun, M.G,G. Zhao and C. Rong (Eds.), CloudCom. LNCS 5931, Springer-Verlag, Berlin, Heidelberg, pp: 90-106. 2009.

[9] Rizvi, Sam, "Performance analysis of AES and Two Fish Encryption Schemes", International Conference on Communication Systems and Network Technologies.58, 2011.

[10] D. Deepali Rane, "Superiority Two fish over Blowfish", International Journal of Scientific research and management (IJSRM), vol. 4, pp. 2321-3418, 2016.

[11] K. Lakshmi Narayanan, "Performance Evaluation of Cryptographic Algorithms: AES and Blowfish", International Journal of Technology and Engineering Science [IJTES]TM, vol.1,no. 7, pp. 1064-1069. 34. 2013.

[12] Thakur, Jawahar, and Nagesh Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithm ssimulation-based performance analysis", International journal of emerging technology and advanced engineering, pp.6-12. February 2011.

[13] Monika Agrawal and Pradeep Moshra, "A Comparative Survey on Symmetric Key Encryption Algorithm", International Journal on Computer Science and Engineering(IJCSE),2014.

[14] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (IJCA), ISSN:0975– 8887)Vol. 1– No.15, 2010.
[15] SuyashVerma, Rajnish Choubey and RoopaliSoni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, vol.2, no.7, 2012.
[16] Prerna Mahajan and Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network,Web & Security, Volume13, Issue15, Version 1.0, 2013.
[17] Abhishek Joshi, Mohammad Wazid and R. H. Goudarc, "An Efficient Cryptographic Schemefor Text Message Protection against Brute Force and Cryptanalytic Attacks", International Conference on Intelligent Computing, Communication & Convergence(ICCC), 2014.
[18] Ashraf Odeh, Shadi R. Masadeh and Ahmad Azzazi, "A Performance Evaluation of Common Encryption Techniques with Secure Watermark System(SWS)", International Journal of Network Security & Its Applications (IJNSA), Vol.7, No.3, 2015.
[19] A.K. Bermani, T.A. Murshedi, and Z. A. Abod, "A hybrid cryptography technique for data storage on cloud computing", Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, no. 6, pp. 1613-1624, 2021.
[20] E.Y. Baagyere, P. A. N., Agbedemnab, Z. Qin, M. I. Daabo, and Z. Qin, "A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers". IEEEAccess, 8, pp.100438-100447, 2020.
[21] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing", InInventive Communication and Computational Technologies, pp.537-547, Springer, Singapore, 2021.