Identification Of Better Encryption Algorithm in Securing Data

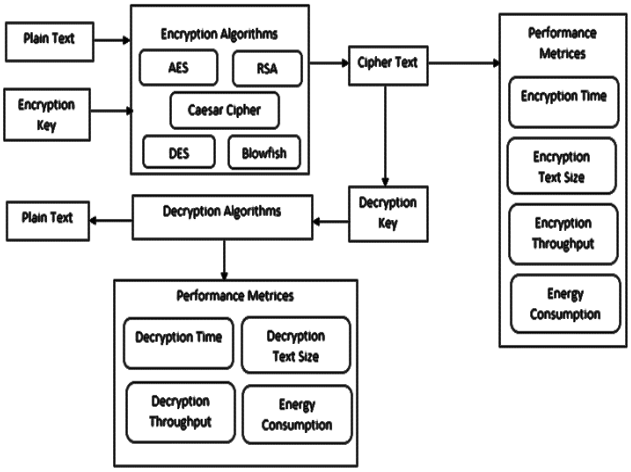
S. Jenifa Sabeena*[1], Dr. S. AntelinVijila[2]

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, India
E-mail: jenifamsu@gmail.com
[2]Assistant Professor, Manonmaniam Sundaranar University, Tirunelveli, India
E-mail: antelinvijila@gmail.com

Abstract
Over the last few years, the usage of the internet has grown considerably in many fields. Data security has become the biggest challenge due to the wide spread usage of the internet. The data that are transferred through the internet or any public network can be easily accessed by unauthorized hackers. One of the best ways to avoid this problem is data encryption. Securing data from unauthorized access is known as encryption which uses many algorithms. Each algorithm has its own strength and weakness. These encryption algorithms are utilized efficiently when it is secure and fast in performance. This work offers a comparative analysis of some widely accepted encryption algorithms such as Advance Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), Blowfish, and Caesar Cipher in terms of data protection, data reliability, scalability, and integrity. Out of these the best one is selected for testing its sustainability. The Brute Force attack and the DOS attack are chosen to test the encryption algorithm.

Keywords: Encryption, decryption, AES, DES, RSA, Caesar Cipher, Blowfish.

Graphical abstract



a. Graphical Abstract

1. INTRODUCTION

Data security is one of the most significant features in the field of data transmission. A high level of security is needed in case of data privacy and storage. It is necessary to implement data protection with a high-security rate and confidentiality. Confidentiality is the process of securing the data from an unauthorized person. Fundamental security service and authentication, integrity, no repudiation, service reliability and

availability are some of the cryptographic goals. The cryptography system ensures better privacy. Hence, to provide confidentiality, many cryptographic algorithms are used. Cryptography is utilized to provide security to the data by preventing it from unauthorized users. The plain text and the ciphertext are the key elements in cryptography. The plain text is the original data and ciphertext is the incomprehensible data formed from the plain text using encryption. The original data must be protected during the process of transmission or storage. Consequently, encryption is utilized for data security.

The encryption algorithm is used to change plain text to cipher text and the decryption algorithm is used to change the cipher text to plain text which is used to secure the data. The key should be kept secret because it is a publicly available algorithm. The sender uses the encryption key to change the plain text to cipher text. The receiver uses the decryption key to change cipher text to plain text. Cryptography is categorized as the symmetric and asymmetric key algorithm. In asymmetric key algorithm, different key is used in the encryption and decryption process. The symmetric key algorithm is further classified into block cipher and stream cipher. AES, DES and Blowfish come under the block cipher. To achieve data security and data privacy, encryption is necessary. The encryption algorithm is used for hiding the original information. The original data is recovered in the decryption process using the decryption key. Encryption is done to protect the original data from unauthorized users. Encryption is also applied in many techniques such as substitution, shifting, or mathematical operations

Ayushi [1] developed a cryptographic method using a symmetric key. It is one of the well-known and fastest algorithms for encryption. The same key is used for encrypting and decrypting data. SuyashVerma et al., [2] developed a cryptographic method using a symmetric key for securing data. It is based on the principle of a block cipher. The performance is evaluated using various plain texts with a single key mode. It is proven that it performs better for same-size data and a single key. PrernaMahajanet et al., [3] have studied AES, DES, and RSA encryption algorithms for data Security. The performance of these encryption algorithms is compared based on time consumption. In some of the approaches, text files are used as input data for evaluating the results. In the research study of Anjula Gupta and Navpreet Kaur Walia [4], various cryptographic algorithms were studied. Several existing encryption algorithms are studied and analyzed to find better encryption algorithms. Finally, it is concluded that the blowfish algorithm performs better in terms of providing high throughput and low power consumption.

The research studies of Rizvi (2011), Deepali Rane (2016) and Lakshmi Narayanan (2013) [5-7], the AES algorithm, blowfish algorithm, and Two Fish algorithm were studied. After the implementation, it is concluded that AES provides better performance than the two fish algorithm. If the RAM size is increased then two fish provides better performance than AES. Two fish results are more efficient than AES in sound and image encryption. When the text size is increased, the efficiency decreases quickly. These approaches also have a low level of security, which varies depending on the PK length and these can be hacked. As a result, Abu-Faraj and Alqadi (2020**)** [8] devised a Highly Secure Data Encryption (HSDE) approach for data quality levels, ensuring that the HSDE destroys data during the encryption stage and recovers the original data during the decryption stage.

Wireless sensor networks (WSNs) are frequently installed in hostile areas with little assistance. It is necessary to provide a particular level of security. The resource limitation is the most significant feature of this network. Hayouni and Hamdi (2020)[9] introduced ULEA, a revolutionary ultra-lightweight encryption method based on Feistel structure. ULEA assumes minimal encryption rounds with reduced transformations and functions to make the cipher complex, in addition to data diffusion and confusion. The Data Encryption Standard (DES) has a key flaw that makes it vulnerable to security risks, but it is widely used due to the speed with which it encrypts and decrypts data. Laia et al., (2020) [10] found that combining the DES algorithm with the Pseudo-random number generator Blum-Blum Shub (BBS) in creating external keys in the encryption and decryption of messages produced a unique key with a high level security.

Single and multiple S-box encryption concerns are examined by Shafique and Ahmed [11]**.**Since, a single S-box replaces the pixels of the same region with a unique symbol.Single S-box encryption fails to encrypt the normal image completely even when replacing a single S-box with several S-boxes improves the image encryption with a large number of grey levels. A dynamic substitution based encryption technique (DSA) is developed to address these challenges, and it is specifically built for highly linked images.

Not only does an encryption algorithm play a crucial part in information security systems, but it also plays a key function in several cloud computing systems. Shukla et al., [12] suggested and analyzed a new encryption-based cloud computing technique. Existing encryption functions are incompatible with real-time applications in embedded systems due to restrictions. In this connection, Hafsa et al., [13] proposed a better cryptographic approach with a high level security and speed. For medical image encryption, an efficient hybrid scheme consisting of an AES-Elliptic Curve Cryptography (ECC),

integrates the benefits of symmetric AES to speed up encryption and asymmetric ECC to secure the exchange of a symmetric session key.

Banani et al., [14] suggested a Dynamic Light-weight Symmetric (DLS) encryption method to handle data protection and secure data transmission in real-time via message marketing. However, Merlin et al., [15] proposed a hybrid encryption and decryption technique that incorporates the concepts of Caesar Cipher and Vigenere Cipher algorithms to reduce the cost of computational resources. Furthermore, this decryption method achieved a 99.99 percent accuracy rate. Encryption methods that rely solely on the S-box are insecure and vulnerable to plaintext and ciphertext assaults. Hence, Munir et al. [16] effectively analyzed an S-box-based encryption system using two different attacks. Only one image is used to execute cryptanalysis in both sorts of assaults.

Furthermore, MUNIR et al. [17] have reported security weaknesses in a recently introduced encryption solution for Internet of Health Things (IoHT) in security based chaotic map to defeat attacks. The approach used a new chaotic map, a modified Mandelbrot set, and a conditional shift algorithm to prove that the encryption algorithm was safe. On the other hand, Crypt analytical approaches have been developed and performed competitively in information security with good outcomes in the development of computer resources. So, in Seth et al., [18], a hybrid cryptographic protocol based on the Blowfish and Paillier encryption algorithms was proposed, and its robustness was compared to the existing hybrid AES and RSA approaches. By reducing calculation time and ciphertext size, the proposed hybrid protocol aims to boost the power of cloud storage.

Reducing the physical space on various storage devices and the time it takes to transport data over the Internet while ensuring that the data is encrypted and hidden from invaders is critical. Therefore, Wahab et al., [19] introduced two techniques with data loss (Lossy) and without data loss (Lossless). To improve security, the hybrid data compression algorithm increases the input data to be encrypted using the RSA process, and it may be utilized to execute lossy and lossless approaches. It can be used to reduce the amount of data sent with each transfer, allowing for faster transmission on slow internet or taking up less space on different storage devices. To prevent interception and alteration, a large amount of data must be encrypted. Although cryptography is used by many individuals regularly, not everyone is aware of it. Xu et al., [20] reviews the use of cryptography in databases and make recommendations for improving security and privacy.

Currently, 5G is displacing its predecessor, and the cloud era is upon us. Research reveals that cloud-based design is the way of the future for IT architecture. If more quantity of data is stored in the cloud, cloud suppliers will be able to collect and analyze user data, but placing one's privacy at risk. Numerous algorithms can be used to calculate the compression ratio. For example, some are lossless, they keep the original data, while others are lossy, and they lose the unique data when compressed. Before concealing the message, it is preferable to employ the cryptographic method for authenticity. Cryptography can make use of a variety of well-known algorithms such as AES, Blowfish, DES, and RSA. Therefore, in this paper, AES, DES, RSA, Blowfish, and Caesar Cipher are analyzed in terms of data protection, data reliability, scalability, and integrity.

The rest of the paper is organized as follows; Section 2 describes the methodology of the proposed techniques, Section 3 describes the result and discussion of the proposed method and it is concluded in Section 4.

2. METHODOLOGY

In this comparative work, best encryption algorithm is selected by finding the performance of AES, DES, Caesar Cipher, Blowfish and RSA. Fig.1 shows the general flow of the comparative work. The input plain text contains 170 records of Vehicle Repair job card details. Encryption is done for the various key values such as 8, 16, 24 & 32. The input data is encrypted and the cipher text is found, then the performance is measured using the metrics such as Encryption time, Encryption throughput and Energy Consumption. Also, the cipher text is decrypted and the performance of these algorithms is measured using the mentioned metrics.

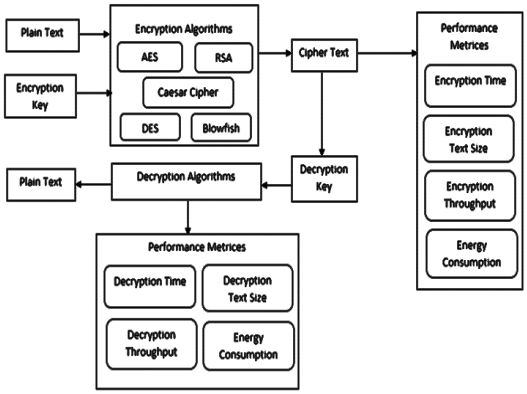


Fig. 1 Comparative Model

2.1 Symmetric Key Algorithm

The same key is used for both encryption and decryption process. This is known as secret-key cryptography. A single key is used for the encryption and decryption process and the cipher text size is smaller or same size. It is used to transfer a large amount of data. The utilization of resources is low and the execution is faster in symmetric key

algorithms when compared to asymmetric key algorithms.

2.1.1 Advance Encryption Standard

AES is known as Rijindeal encryption. Rijindeal (AES) was found by Joan Daemen & Vincent Rijman in1999 [21]. It is a symmetric block cipher algorithm. Here the same key is used for both encryption and decryption process. The plain text and the cipher text size should be the same. That is if the data length is 128, 192, 256-bits then the length of the key should be 128, 192, 256-bits.

2.1.2 Data Encryption Standard

Data Encryption Standard was developed by IBM in the year 1970 and submitted to NBS to check the strength and security of the algorithm. The algorithm 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 halves of the data is called a permutation. This form of the structure is called the Substitution and Permutation Network (SPN).

2.1.3 Caesar Cipher

Caesar cipher is a kind of substitution cipher which follows symmetric encryption methods. It is a widely used encryption algorithm. It is named after Julius Caesar, who used this to communicate with his officials. In this type, each cipher letter is created by the plain text letter by another letter to some fixed number of positions. For both the encryption and decryption process, the value of the shift key and reference table of alphabets and their numerical equivalent are needed.

2.1.4 Blowfish

In the year 1993, Bruce Schneier [22] designed the blowfish algorithm. Blowfish is one of the symmetric-based block cipher-based algorithms which have the same key that will be used for both the encryption function and decryption function. The block cipher principle is that the plain text and the cipher text size must be same. The blowfish algorithm encrypts a 64-bit block with a variable length key [32 to 446-bits]. The number of sub-keys generated is 18 [P- array] and it takes 16 rounds for processing. It has 4 S-boxes with each substitution box having 12 entries of 32-bits.

2.2 Asymmetric Key Algorithm

The encryption and decryption processes are performed using different keys. This is known as the public key cryptography and the working principle is the opposite of symmetric key algorithm. Two different keys namely the public key and a private key are needed for asymmetric key algorithm. For encryption, public key is used and for the decryption process, the private key is used. A public key can be given to anyone and a private key is kept private. Some of the asymmetric key algorithms are RSA, DSA, Diffie Hellman, etc.

2.2.1 RSA (Rivest-Shamir-Adleman)

In 1997 RSA was introduced by Rivest, Shamir, Adleman. It is a type of block-cipher algorithm, where the plain text is converted to cipher text. It uses a public key for encryption and a private key for decryption. Mathematical formulas are used in RSA to convert the plain text into cipher text and vice versa.

2.3 Comparative Analysis on Existing Algorithms

The comparison of this cryptographic algorithm highlights the strength and weakness of the encryption methods, the algorithm structure, length of the key and the total rounds for each encryption algorithm. Table 1, shows the comparison of symmetric and asymmetric algorithms.

Scalability means the capacity to what extent the information can be changed in size or scale. DES and Blowfish algorithm are scalable as they have the Feistel structure. The RSA algorithm has high power consumption as the computation time for this algorithm is very high when compared to other algorithms. The Caesar Cipher algorithm has inadequate security and the RSA algorithm provides high security for the user data. RSA algorithm is tunable as it is asymmetric. The cryptanalysis resistance is checked using the brute force attack and DoS attack.

Table 1. Comparison of Symmetric and Asymmetric Algorithms

Factors	AES	DES	Blowfish	Caesar Cipher	RSA
Developed By	Joan Daemen, Rijman in1998	IBM in 1970	Bruce Schneier in 1993	Julius Caesar	Rivest, Shamir, Adleman in 1977
Algorithm Structure	Substitution-Permutation	Feistel	Feistel	Substitution	Use Public and Private key
Key Length	128,192 and 256-bits	56-bits	32 to 448-bits	Number of shifts = 0 – 25	1024-bits
No. of Rounds	10,12,14	16	16	Traditionally 3	No Rounds
Cipher Type	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric
Scalability	No	Yes	Yes	No	No
Consumption of power	Low	Low	High	Low	Very High
Security	High	High	High	Inadequate	Secure for user only
Tunablity	No	No	No	No	Yes
Cryptanalysis Resistance	Strong	Vulnerable	Vulnerable	Vulnerable	Brute Force attack difficult to accomplish

3. RESULTS AND DISCUSSION

The cryptographic algorithms are implemented in Python. The algorithms have been tested on the system configuration Intel(R) Pentium(R)CPU, 4GB RAM, 64bit Operating System, x64- based processor. The results of the AES, DES, Caesar Cipher, Blowfish, and RSA algorithms are shown in Table 2, Table 3, Table 4, Table 5, and Table 6, respectively.

The results of various algorithms in terms of encryption time, decryption time, total time, encryption throughput, decryption throughput, energy concerning input data with text size 19970 and different key sizes are shown.

Table. 2. Performance of AES

Algorithm	AES			
Input Data	170	170	170	170
Text Size	19970	19970	19970	19970
Key size	8	16	24	32
Encryption Time in ms	8.96	35.45	53.99	39.29
Decryption Time in ms	0.015	1	1	1
Total Time in ms	8.98	36.45	54.99	40.29
Encryption Throughput	0.189	0.047	0.031	0.043
Decryption Throughput	109.59	1.7	1.7	1.7
Energy in Joules	112.11	443.15	674.97	491.19

Table 2 represents the performance of AES algorithm for different key sizes 8, 16, 24 and 32.

Table. 3. Performance of DES

Algorithm	DES			
Input Data	170	170	170	170
Text Size	19970	19970	19970	19970
Key size	8	16	24	32
Encryption Time in ms	0.031	0.124	0.125	0.171
Decryption Time in ms	0.046	0.124	0.124	0.156
Total Time in ms	0.078	0.249	0.25	0.328
Encryption Throughput	56.32	14.08	14.05	10.24
Decryption Throughput	36.26	13.6	13.6	8.573
Energy in Joules	0.39	1.562	1.564	2.148

Table 3 represents the performance of DES algorithm for different key sizes 8, 16, 24 and 32.

Table 4. Performance of Caesar Cipher

Algorithm	CAESAR CIPHER			
Input Data	170	170	170	170
Text Size	19970	19970	19970	19970
Key size	8	16	24	32
Encryption Time in ms	1	1	1	1
Decryption Time in ms	1	1	1	1
Total Time in ms	2	2	2	2
Encryption Throughput	1.7	1.7	1.7	1.7
Decryption Throughput	1.7	1.7	1.7	1.7
Energy in Joules	12.5	12.5	12.5	12.5

Table 4 represents the performance of Caesar Cipher algorithm for different key sizes 8, 16, 24 and 32.

Table 5. Performance of Blowfish

Algorithm	BLOWFISH			
Input Data	170	170	170	170
Text Size	19970	19970	19970	19970
Key size	8	16	24	32
Encryption Time in ms	0.015	1	1	1
Decryption Time in ms	0.078	0.078	0.078	0.078
Total Time in ms	0.093	1.078	1.078	1.078
Encryption Throughput	80.47	0.07	0.08	1.4
Decryption Throughput	22.53	22.52	22.52	22.52
Energy in Joules	0.195	12.5	12.5	12.5

Table 5 represents the performance of blowfish algorithm for different key sizes 8, 16, 24 and 32.

Table 6.Performance of RSA

Algorithm	RSA			
Input Data	170	170	170	170
Text Size	19970	19970	19970	19970
Key size	8	16	24	32
Encryption Time in ms	10.686	8.765	5.531	8.281
Decryption Time in ms	2.593	0.125	31.93	49.88
Total Time in ms	13.28	8.89	37.46	58.16
Encryption Throughput	0.943	1.148	2.127	1.557
Decryption Throughput	0.655	13.59	0.0532	0.034
Energy in Joules	133.58	109.56	69.13	103.51

Table 6 represents the performance of RSA algorithm for different key sizes 8, 16, 24 and 32.

3.1 Encryption Time

The time taken for converting the plain text into cipher text is called the encryption time. It is based on the size of the key and block which is in milliseconds. Fig.2 shows the bar chart of encryption time in the cryptographic algorithms.

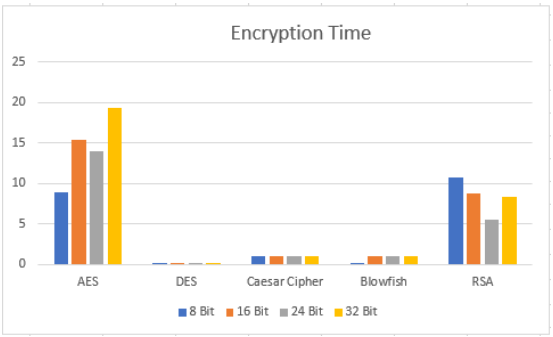


Fig. 2 Encryption Time

3.2 Decryption Time

The time taken for converting the cipher text in to plain text is the decryption time. It is also represented in milliseconds. Fig.3 shows the bar chart of decryption time in the cryptographic algorithms.

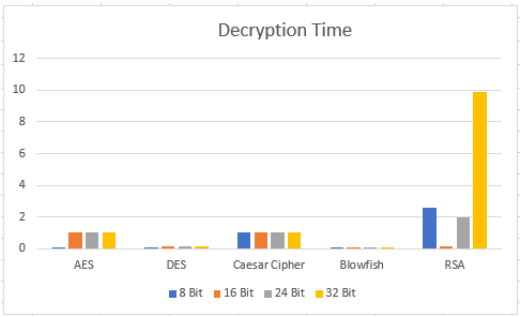


Fig. 3 Decryption Time

3.3 Encryption Throughput

The encryption throughput is calculated using a total number of data blocks successfully transferred and the time taken for encryption is measured in terms of seconds. The throughput is used to measure the data transfer rate.

$$Encryption\_Throughput = \frac{Tn_p}{En_t} \quad (1)$$

Where,

Tn_p = Total number of plain text (bytes)

En_t = Encryption time measured in terms of seconds.

Fig.4, shows the bar chart of encryption throughput in the cryptographic algorithms.

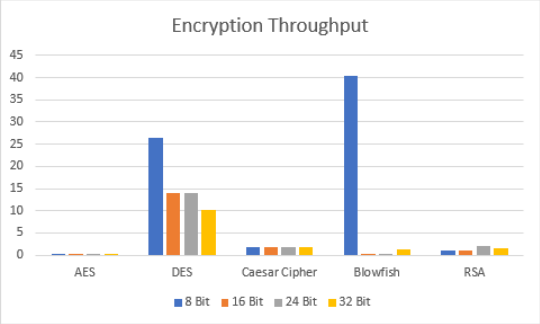


Fig. 4 Encryption Throughput

3.4 Decryption Throughput

The decryption throughput is calculated using the total number of successfully transferred data blocks (cipher text in bytes) divided by the time taken (decryption time in seconds). Fig.5 shows the bar chart of decryption throughput in the cryptographic algorithms.

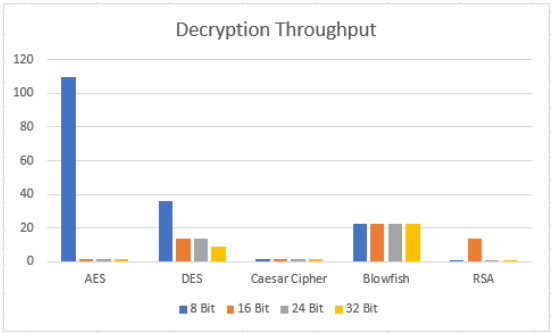


Fig. 5 Decryption Throughput

3.5 Time Consumption

The time taken for encryption and decryption is calculated using the time needed for finishing the key generation. Fig.6 shows the bar chart of time consumption in the cryptographic algorithms.

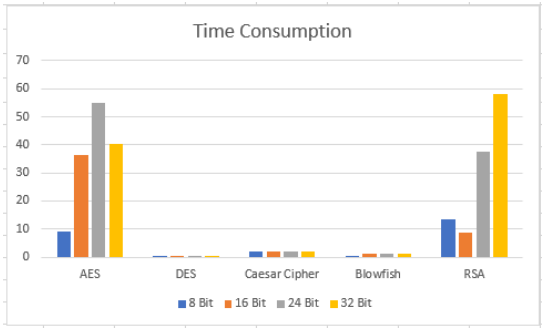


Fig. 6 Time Consumption

3.6 Energy Consumption

The energy consumed for the encryption process is calculated by the number of clock cycles needed for the completion of encryption and the average current haggard for each of the CPU clock cycles.

$$E = V_{cc} \times I \times N \times \tau \quad (2)$$

Where,

V_{cc}= supply voltage of the system,

I = average current drawn from power source

N = number of clock cycles, τT = clock period

T = N/ processor speed (seconds)

Fig.7 shows the bar chart of energy consumption in the cryptographic algorithms.

4. CONCLUSION

The encryption algorithms such as AES, DES, RSA, Blowfish and Caesar Cipher are analyzed in the vehicle repair job card details and compared in this work. These algorithms prevent the data from brute force and denial of service attacks. Each encryption algorithm has its strength and weakness. From this analysis, it is clearly understood that the RSA encryption algorithm is better in security but takes more time for processing and more memory space. So, it is concluded to utilize the DES algorithm for encryption and decryption process whereas RSA can be applied for key exchange. The performance of the encryption algorithms has been compared with several parameters primarily including time, energy and throughput. For providing security to better data encryption algorithms can be found by combining the existing encryption algorithms. Multiple levels of security can be given to protect data instead of single-level security.

ACKNOWLEDGEMENT

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. Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887) Vol. 1 – No. 15, February 2010.
2. Suyash Verma, 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, Volume 2, Issue 7, July 2012.
3. 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, Volume 13, Issue 15, Version 1.0, Year 2013.
4. Anjula Gupta and Navpreet Kaur Walia, "Cryptography Algorithms: A Review", International Journal of Engineering Development and Research, IJEDR Volume 2, Issue 2, ISSN: 2321-9939, 2014.
5. Rizvi, "Performance analysis of AES and TwoFish Encryption Schemes", International Conference on Communication Systems and Network Technologies. 58, 2011.
6. DeepaliRane, "Superiority Twofish over Blowfish", International Journal of Scientific Research and Management (IJSRM), vol. 4, pp. 2321-3418, D 2016.
7. 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, K 2013.
8. Abu-Faraj and Alqadi, " Using Highly Secure Data Encryption Method for Text File Cryptography", International Journal of Computer Science & Network Security, vol. 21, no. 12, pp. 53-60, 2021.
9. Hayouni and Hamdi," A novel energy-efficient encryption algorithm for secure data in WSNs", The Journal of Supercomputing, vol. 77, no. 5, pp. 4754-4777, 2021.
10. Laia and Zamzami, "Analysis of Combination Algorithm Data Encryption Standard (DES) and Blum-Blum-Shub (BBS)," In Journal of Physics: Conference Series, vol. 1898, no. 1, pp. 012017). 2021.
11. Shafique and Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," Multidimensional Systems and Signal Processing, vol. 32, no. 1, pp. 91-114, 2021.
12. Shukla, Dwivedi, and Trivedi, "Encryption algorithm in cloud computing", Materials Today: Proceedings, vol. 37, pp. 1869-1875, 2021.
13. Hafsa, Sghaier, Malek, and Machhout, "Image encryption method based on improved ECC and modified AES algorithm", Multimedia Tools and Applications, vol. 80, no. 13, pp. 19769-19801, 2021.
14. Banani, Thiemjarus, Wongthavarawat, and Ounanong, "A Dynamic Light-Weight Symmetric Encryption Algorithm for Secure Data Transmission via BLE Beacons", Journal of Sensor and Actuator Networks, vol. 11, no. 1, pp.2, 2021.
15. Tan, Arada, Abad, and Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher", In Journal of Physics: Conference Series, vol. 1997, no. 1, p. 012021, 2021.
16. Munir, Khan, Shah, Alanazi, and Hussain, "Cryptanalysis of nonlinear confusion component based encryption algorithm", Integration, vol. 79, pp. 41-47, 2021.
17. Munir, Khan, Hazzazi, Aijaedi, Alharbi, and Hussain, "Cryptanalysis of internet of health things encryption scheme based on chaotic maps", IEEE Access, vol. 9, pp. 105678-105685, 2021.
18. Seth, Dalal, Le, Jaglan, Dahiya, Agrawal, and Verma, "Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm", CMC-COMPUTERS MATERIALS & CONTINUA, vol. 67, no.1, pp.779-798, 2021.
19. Wahab, Khalaf, Hussein, and Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques", IEEE Access, vol. 9, pp.31805-31815, 2021.
20. Xu, Thakur, Kamruzzaman, and Ali, "Applications of Cryptography in Database: A Review", In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1-6). 2021.
21. Daemen and Rijmen, "AES proposal: Rijndael", 1999.
22. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)", In International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, pp. 191-204,1993.