Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Blended BFD Symmetric Encryption Algorithm

Uma Maheswari. K
Research Scholar (VISTAS,Pallavaram)
Assistant Professor (A.M. Jain College)
Chennai, India.
umasaravanan.k@gmail.com

Dr. V. Sumalatha
Associate Professor (VISTAS, Pallavaram)
Chennai,India.
Sumalatha.scs@velsuniv.ac.in

Abstract

As companies started moving into cloud services, data security has become the utmost concern for them. Even though strict protocols are being followed in cloud platforms, it is important to use an independent encryption method during data transfer and storage. Blowfish-DES is an attempt to address it. This algorithm is a hybrid of Blowfish and DES, giving us the best of both worlds when it comes to data security without sacrificing processing speed. Keywords—algorithm, cloud platforms.

I. INTRODUCTION

Cloud security is crucial because most firms are currently adopting cloud computing in some way or another. According to Gartner, the global market for public cloud services will grow 17% by 2020, with software as a service (SaaS) continuing to be the largest sector. [1] "Cloud adoption is now widespread," says Gartner research vice president Sid Nag. However, as more data and apps are moved to the cloud, IT professionals are concerned about security, governance, and compliance challenges when their content is transmitted or kept there. [14] They are concerned that extremely sensitive corporate information and intellectual property could be compromised as a result of unintentional leaks or more sophisticated cyber assaults.

Cloud security includes safeguarding data and company information such as client orders, sensitive design blueprints, and financial records. Data breaches and theft must be avoided at all costs in order to maintain consumer trust and protect the assets that contribute to your competitive advantage. [9] Businesses may realise the benefits of cloud computing by maintaining a robust cloud security posture, which include fewer upfront costs, lower ongoing operational and administrative costs, ease of scaling, higher reliability and availability, and an entirely new way of working.

II. ENCYPTION METHODS IN CLOUD SECURITY

Encryption is the process of encrypting data in such a way that it can only be accessed by authorised parties. During the encoding process, plain text is turned to cypher text. To decrypt the cypher text, we'll need a decryption key. Depending on the key used for encryption and decryption, encryption methods are classed as symmetric or asymmetric. [1]

A. Symmetric Encryption Methods

This method uses same key for both encryption and decryption. Symmetric encryption methods include block cypher and stream cypher. In the block cypher approach, data is encoded or decoded with blocks of plain text or cypher text, whereas in the stream cypher method, data is encoded or decoded with each letter. [4]

The most extensively used symmetric encryption algorithms areAES (Advanced Encryption Standards), Triple DES (3- Data Encryption Standards), IDEA (International Data Encryption Algorithm), Blowfish, and

Twofish. [5] [16] For encrypting data at rest or in private channels like databases and banking transactions, symmetric encryption algorithms are the best option. [2]

B. Asymmetric Encryption Methods

For encryption and decryption, asymmetric encryption systems employ two independent keys: a public key for encryption and a private key for decryption. The most extensively used asymmetric encryption technologies are the RSA and ECC algorithms. Asymmetric encryption algorithms are used in digital signatures, blockchain, and public-key infrastructure (PKI). [2] [5]

III. METHODOLOGY

This encryption method is a hybrid of Blowfish and single DES. We can take use of the speed and power of both algorithms by merging them. Blowfish-DES is a symmetric encryption technique, which means it encrypts and decrypts messages using the same secret key. [3] It is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption.

A. Blowfish Algorithm

This method is based on the festal structure, which effectively converts any function to a permutation. It uses a 64-bit block size and generates keys with lengths ranging between 32 and 448 bits.[3] There are two parts to this method. The first is to encrypt data, and the second is to enlarge the key.

The key expansion transforms the 448 bits of a key into subkeys once it receives the request, making the array 4168 bytes long. The algorithm now employs a 16-round Feistel cypher as well as big key-dependent S-boxes for data encryption. S-boxes are necessary components of symmetric key algorithms that use the substitution approach. [9]

The permutation key for each cycle of substitution in the S-boxes is different. The algorithm follows the same structure as CAST-128, which uses fixed S-boxes. We should use the same structure to decode the blowfish technique once we constructed the encryption structure. It's because the Feistel structure cypher theory underpins the Blowfish cypher. [14] Each half of the plain text is saved either alone or with a round key using the F function's output. Furthermore, the switches on the halves' sides have no influence on the halves' worth.

B. DES Algorithm

In DES, a 56-bit key is employed. The first key has a length of 64 bits. However, before the DES process even starts, every eighth bit of the key is destroyed, resulting in a 56-bit key. This method eliminates bit locations 8, 16, 24, 32, 40, 48, 56, and 64. As a result, eliminating every 8th bit from a 64-bit key generates a 56-bit key. Substitution (also known as confusion) and transposition are two cryptographic fundamentals that DES is built on (also called as diffusion). DES consists of 16 rounds, each of which is referred to as a step. [15] Each round includes substitution and transposition. [3]

IV. IMPLEMENTATION

A. Encryption

- The 208-bit key is passed along with the plain text into the function.
- The key is divided into two halves. One half for DES and other half for Blowfish.
- DES key is 64 bits(K1) and 144 bit key(K2) for Blowfish.
- Plain Text is passed into the DES block along with key (K1).

V. EVALUATION

- This 64 bit block of plain text is passed into initial permutation where bit positions are swapped as below.

Table 1. Initial permutation Table

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

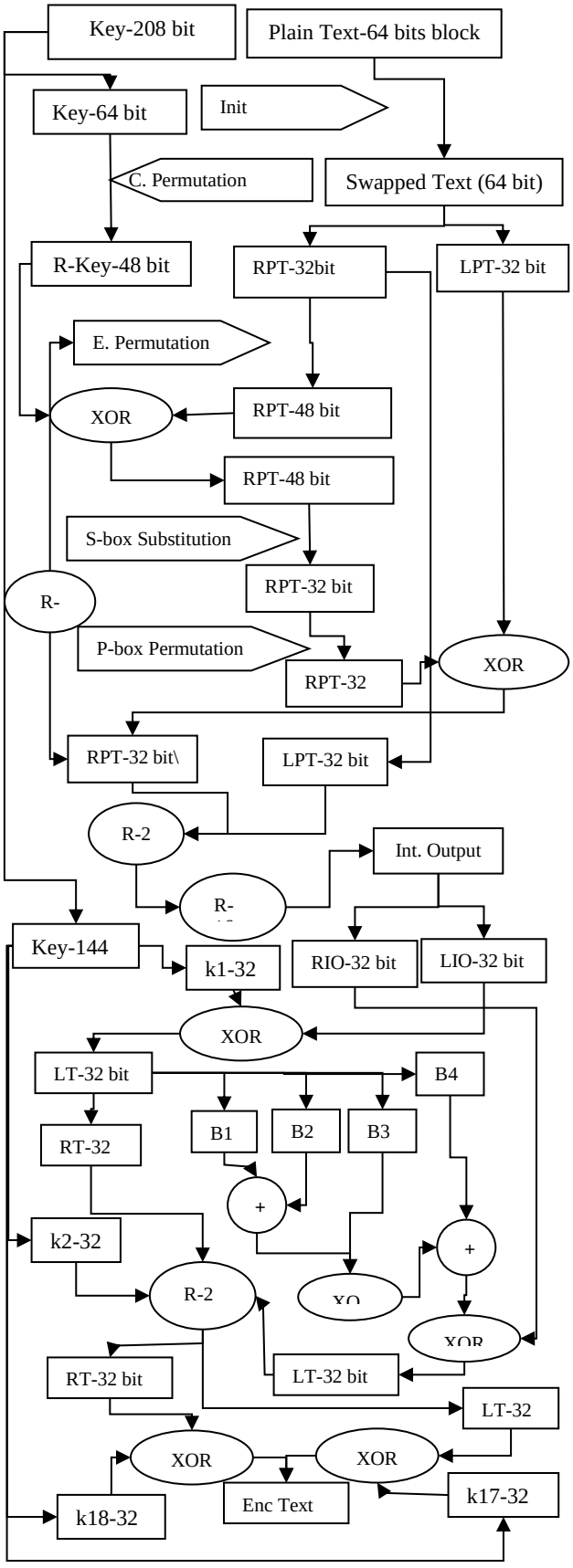
- The resulting output is divided into two halves i.e. Left Plain Text and Right Plain Text each of 32 bit which will goes through 16 rounds of function F .
- A technique called Compression Permutation generates a new key (R-key) of 48 bits for each round, where bits are shifted left by 1 position for rounds 1,2,9,16 and 2 positions for the remaining rounds selecting 48 bits.
- Now, in each round, a function F is called, which expands right plain text from 32 bits to 48 bits using a process known as Expansion Permutation, in which 32 bits are divided into 8 blocks, each block of 4 bits, and each block is expanded to 6 bits by joining the outermost bits from adjacent blocks. [12] After that, the output 48 bit is XORed with a 48 bit round key.
- The 48-bit output is then processed via the S-box substitution, which divides the 48-bit XOR output into eight 6-bit blocks, each of which produces a 4-bit output. As a result, the 48-bit output is reduced to a 32-bit value.
- The value is then sent to a P-box permutation, which results in bit transposition. The P-box permutation's output is XORed with Left plain text and used as right plain text input for the following round, while the right plain text from this round is used as left plain text in the next round.
- The above step is repeated for 16 times. The final left plain text and right plain text are joined and pushed into final permutation step.
- The output from this permutation step is passed into blowfish algorithm where the 64 bit blocks of the text are split again into left text and right text each 32 bit.
- Now the key (K2) is processed to create 18 sub keys(round keys) each of length 32 bit for 16 rounds of encryption.[10]
- The left text in round 1 is XORed with round key 1. The result is then passed to a procedure that divides a 32-bit block into four 8-bit blocks.
- Each block is fed into the S-Box expansion, which generates 32-bit output. The outputs of the first and second blocks are summed and XORed with the output of the third block, which is then summed with the output of the fourth block.
- This 32-bit output is XORed with right text and passed to the next round as left text. The result of XORing the left text of this round with the round key is transferred to the following round as the right text.
- The above step is repeated for 16 times and the final left and right texts are XOR ed with round key 17 and round key 18 respectively.

The outputs from the above step is joined together as an encrypted text.

A. Decryption

The steps involved in the encryption is done in reverse order to get the decrypted text. The encrypted text is processed to get the decrypted plain text.

B. *lowchart*


Key-208 bit
Plain Text-64 bits block
Key-64 bit
Init
C. Permutation
Swapped Text (64 bit)
R-Key-48 bit
RPT-32bit
LPT-32 bit
E. Permutation
XOR
RPT-48 bit
RPT-48 bit
S-box Substitution
RPT-32 bit
R-
P-box Permutation
RPT-32
XOR
RPT-32 bit\
LPT-32 bit
R-2
Int. Output
R-
Key-144
k1-32
RIO-32 bit
LIO-32 bit
XOR
LT-32 bit
B4
RT-32
B1
B2
B3
+
k2-32
+
R-2
XO
XOR
RT-32 bit
LT-32 bit
LT-32
XOR
XOR
k17-32
Enc Text
k18-32

VI. EVALUATION

To compare Blowfish-DES with AES and triple-DES algorithms a dataset is prepared with a list of string with bytes size varying from 1 byte to 1000 bytes.[17] The whole dataset was passed onto the algorithms one by one and time taken for encryption and decryption were recorded. The recordings were plotted in a graph

VII. FIGURES AND TABLES

The algorithm is compared against AES and Triple DES algorithms in terms of its speed while encryption and decryption.

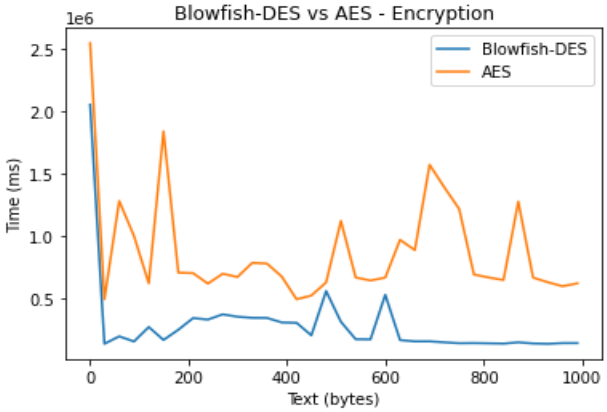


Fig.1. Time taken for encryption Blowfish-DES vs AES

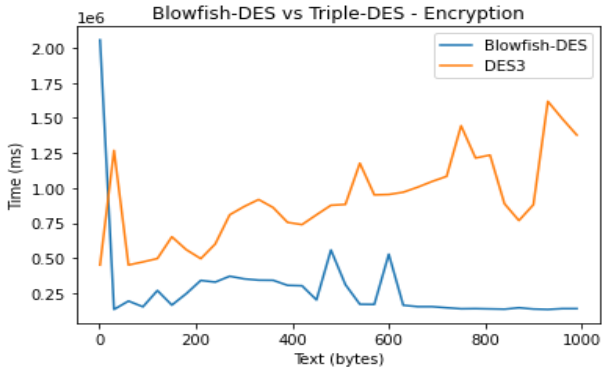


Fig.2.Encryption Time. Blowfish-DES vs Triple DES

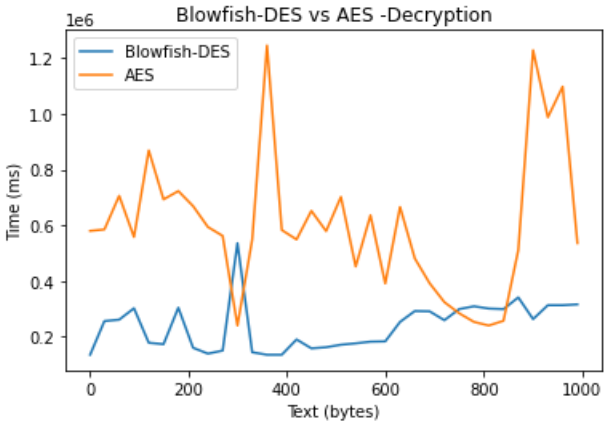


Fig.3. Decryption Time. Blowfish-DES vs AES

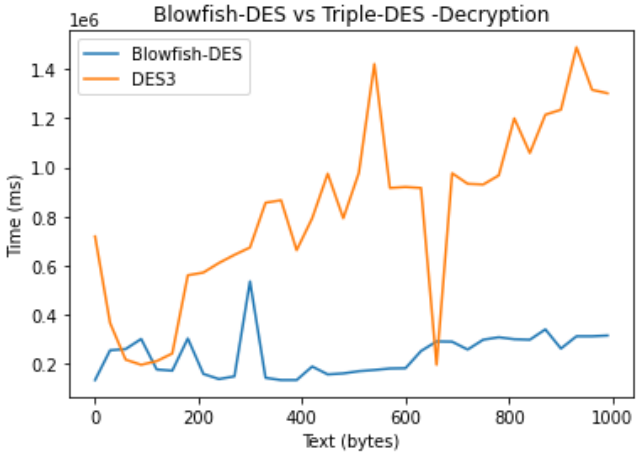


Fig.4. Decryption Time. Blowfish-DES vs Triple DES

Table 2. Average Time Taken - Encryption

	Blowfish-DES	AES	Triple-DES
Average Time (milliseconds)	0.21	0.82	0.93

Table 3. Average Time Taken -Decryption

	Blowfish-DES	AES	Triple-DES
Average Time (milliseconds)	0.23	0.68	1.2

VIII. CONCLUSION

When compared to Triple-DES, the method yields a linear curve with substantially lower changes when tested with the dataset. AES provides a curve that is comparable to Blowfish-DES, implying that both algorithms take the same amount of time to process any length of text block. The exponential curve found in the Triple-DES approach suggests that processing time increases exponentially with increasing byte size of the text. Both encryption and decryption take less time with Blowfish-DES. As a result, it's ideal for data transfer in situations when speed is critical.

REFERENCE

[1] Gupta, Anjula & Walia, Navpreet. (2014). Cryptography Algorithms: A Review. International Journal of Engineering Development and Research 2321-9939. 2. 1667.

[2] Naik, Rasika & Lathi, Anand & Pariani, Siddhant & Satpute, Namrata & Singh, Ankita. (2021). Comparison of Different Encryption Algorithm and Proposing an Encryption Algorithm. SSRN Electronic Journal. 10.2139/ssrn.3867982.

[3] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," P rocedia Computer Science, vol. 78, pp.617–624, Jan. 2016, htt ps://doi.org/10.1016/j.procs.20 16.02.108

[4] ABIODUN, Ahmida & LAWAL, Olanrewaju & OYEBIYI, Oyediran & JOSEPH, Odiete & ADETORO, Adeyemi. (2021). Performance Evaluation of Selected Encryption Algorithms. International Journal of Information Security and Cybercrime. 10. 21-30. 10.19107/IJISC.2021.02.03.

[5] Gyawali, Yashant & Subedi, Bijayraj. (2020). ENCRYPTION ALGORITHM Advanced Encryption Standard.

[6] Iftikhar, U. & Asrar, K. & Waqas, M. & Ali, S.. (2021). Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices. Engineering, Technology & Applied Science Research. 11. 7867-7874. 10.48084/etasr.4263.

[7] Muin, Muhammad & Setyanto, Arief & Sudarmawan, & Santoso, Kartika. (2018). Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations. 137-141. 10.1109/ICITACEE.2018.8576929.

[8] Gangireddy, Venkata & Kannan, Srihari & Subburathinam, Karthik. (2021). Implementation of enhanced blowfish algorithm in cloud environment. Journal of Ambient Intelligence and Humanized Computing. 12. 10.1007/s12652-020-01765-x.

[9] Quilala, Theda Flare & Sison, Ariel & Medina, Ruji. (2018). Modified Blowfish Algorithm. Indonesian Journal of Electrical Engineering and Computer Science. 12. 38-45. 10.11591/ijeecs.v12.i1.pp38-45.

[10] Lokhande, Mukul & Khake, Naresh. (2020). Verilog Implementation of AFS algortihm.

[11] Siahaan, Andysah Putera Utama. (2018). Encryption of DES Algorithm in Information Security. 10.31227/osf.io/d9p6b.

[12] Ortakci, Yasin & Abdullah, Mohammed. (2021). Performance Analyses of AES and 3DES Algorithms for Encryption of Satellite Images. 10.1007/978-3-030-66840-2_67.

[13] Aleisa, Noura. (2015). A comparison of the 3DES and AES encryption standards. International Journal of Security and Its Applications. 9. 241-246. 10.14257/ijsia.2015.9.7.21.

[14] Commey, Daniel & Griffith, Selorm & Dzisi, James. (2020). Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage. International Journal of Computer Applications. 177. 17-22. 10.5120/ijca2020919897.

[15] Pande, Sagar. (2014). An Information Security Scheme for Cloud based Environment using 3DES Encryption Algorithm. International Journal of Recent Development in Engineering and Technology. 2. 65-68.

[16] Maharaj, Ashutosh. (2020). A Review on Advanced Encryption Standards (AES).

[17] Sousi, Ahmad-Loay & Yehya, Dalia & Joudi, Mohamad. (2020). AES Encryption: Study & Evaluation.