International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 77-82 DOI: https://doi.org/10.63671/ijsssr.v4i1.493
Volume: 4 | Issue: 1
April-June 2026

Security In Cloud Computing Using Blow Fish Algorithm

Dr. Sivasakthi

Vanita Vishram Women's University, Surat, India

Author Email: shakthiannmalai4@gmail.com

Abstract— Cloud computing is a resource pool with a huge number of machines that stores massive amounts of data. Encryption techniques can be used to secure massive amounts of data in the cloud. Recent years, increase in the mobile devices and cloud processing the data stored in the cloud in the form of pictures, messages and texts. Cloud services used by the clients. For enchancing the security in the cloud, new cyber security model is introduced with optimal key selection. Encryption is a technique used for converting data into encrypted data and securely transmitting data over public networks. The data is encrypted and stored in the cloud using blow fish encryption. To improve the accuracy and protecting confidential information from illegal access. In this paper we discussed about block-based transformation approach that combines data with the blow fish encryption algorithm. We also examined cloud computing security difficulties, applications that use this algorithm for secured data transmission, and as well as a metaphoric analysis of the blow fish security algorithm.

Keywords: Cloud computing, Blow fish algorithm, DES algorithm, AES algorithm, Encryption, Decryption.

I. INTRODUCTION

I.I. CLOUD COMPUTING

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, and analytic—over the internet ("the cloud") rather than using local servers or personal devices. This allows users and businesses to access, store, and manage data and applications on-demand, without needing to invest in or maintain physical infrastructure.

The four main types of cloud computing deployment models are: public, private, hybrid, and community clouds.

I.II. PUBLIC CLOUD

Infrastructure is owned and managed by a third-party provider and is accessible to the general public or a large community.

I.III. PRIVATE CLOUD

Infrastructure is dedicated to a single organization and can be managed internally or by a third-party provider, offering greater control and security.

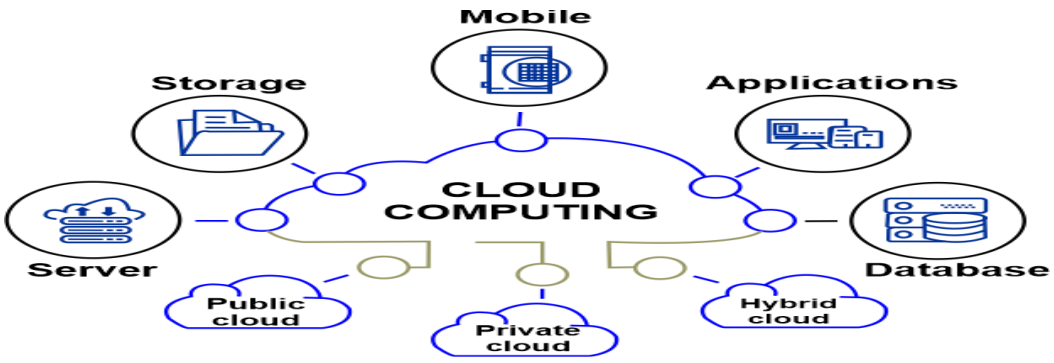
I.IV. HYBRID CLOUD

Combines public and private cloud resources, allowing organizations to choose the best environment for different workloads.

I.V. COMMUNITY CLOUD

Infrastructure is shared by multiple organizations with common interests or requirements, but is still managed by a third-party provide.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 77-82 DOI: https://doi.org/10.63671/ijsssr.v4i1.493
Volume: 4 | Issue: 1
April-June 2026



1.1 cloud Computing

I.VI. KEY FEATURES OF CLOUD COMPUTING

On-demand self-service: Users can provision and manage resources as needed, without requiring human intervention from the service provider.

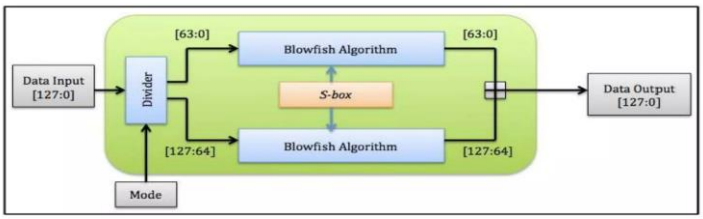
Broad network access: Cloud services are accessible over the internet, allowing users to connect from various devices, such as computers, smartphones, and tablets.

II. BLOWFISH ALGORITHM (SYMMETRIC)

Overview: Blow-fish is a fast, symmetric encryption algorithm developed by Bruce Schneier. It is known for its key flexibility (supports key sizes ranging from 32 bits to 448 bits).

3. BLOWFISH ALGORITHM

The blowfish algorithm is having plaintext range of 128 bit and variable key length from 32 bits to 448 bits and it performs 16 rounds of operations.



II.I. HOW IT WORKS

Key Expansion: A key is used to generate several sub-keys that are stored in a P-array and S-boxes. These sub-keys are used during the encryption process.

Rounds: Blow-fish divides the data into 64-bit blocks and encrypts it over 16 rounds. Each round applies several transformations, including substitution (using S-boxes) and permutation (using XOR and shifts).

Final Output: After all rounds, the data becomes cipher-text.

II.II. STRENGTHS

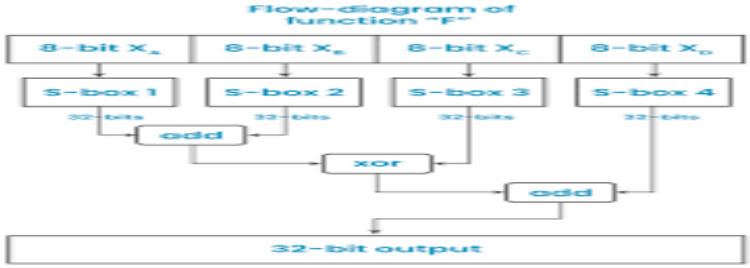
Blow-fish is fast and highly secure with a variable key length.

It's resistant to most common crypt analytic attacks.

II.III. WEAKNESSES

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 77-82 DOI: https://doi.org/10.63671/ijsssr.v4i1.493
Volume: 4 | Issue: 1
April-June 2026

The 64-bit block size can be a limitation compared to modern algorithms (e.g., AES uses 128-bit blocks).



II.IV. WORKING OF BLOWFISH ALGORITHM

Blowfish uses a **Feistel network structure** with **16 rounds of encryption**.

II.V. STEPS: KEY EXPANSION

The secret key is converted into several subkeys.

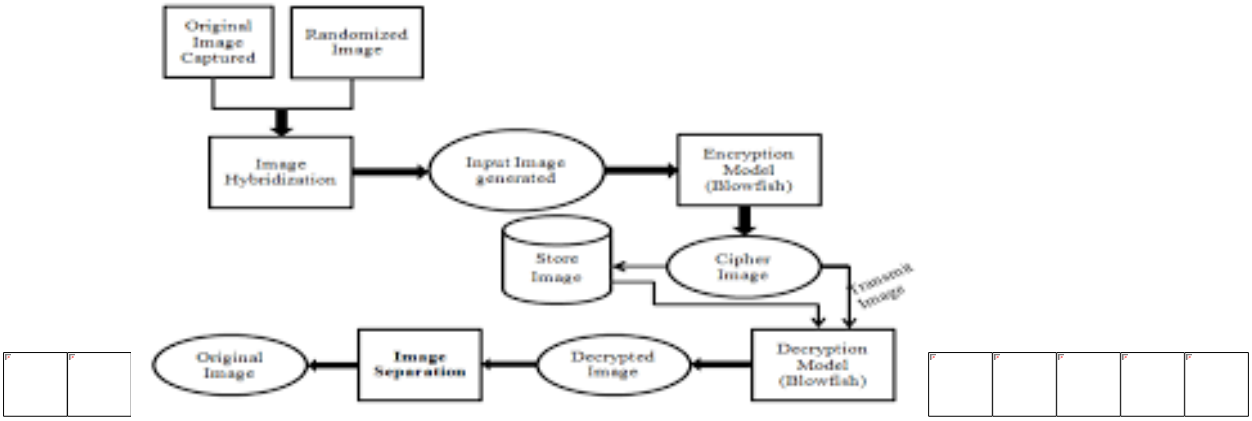
Generates **P-array (18 subkeys)** and **four S-boxes**.

II.VI. DATA DIVISION

Plaintext is divided into **64-bit blocks**.

II.VII. FEISTEL ROUNDS (16 ROUNDS)

- ❖ Each round performs:
- ❖ XOR operation
- ❖ Substitution using S-boxes
- ❖ Swapping of left and right halves.



II.VIII. FINAL TRANSFORMATION

After the 16th round, the two halves are swapped and combined to produce cipher-text.

A. Blow-fish in Cloud Computing

B. In cloud environments, Blow-fish is used for:

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 77-82 DOI: https://doi.org/10.63671/ijsssr.v4i1.493
Volume: 4 | Issue: 1
April-June 2026

- ✓ Data encryption before storing files in cloud storage
- ✓ Securing data transmission between client and cloud server
- ✓ Protecting sensitive information like passwords and financial data
- ✓ Database security in cloud systems

Example:
Before uploading a file to cloud storage, the file is **encrypted using Blow-fish**, so even if attackers access the data, they cannot read it without the key.

III. AES ALGORITHM (SYMMETRIC)

Overview: AES is widely considered the gold standard in encryption and is used in everything from securing websites to government communication. It operates on 128-bit blocks and supports key sizes of 128, 192, or 256 bits.

III.I. HOW IT WORKS

Rounds: AES performs multiple rounds of encryption. The number of rounds depends on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

Transformations: AES uses substitution (S-box), permutation (shift rows), and mixing (mix columns) in each round, followed by adding the round key.

III.II. STRENGTHS

AES is very efficient, highly secure, and widely used in various security protocols.

III.III. WEAKNESSES

Requires significant computational power for large datasets compared to simpler algorithms like Blowfish.

III.IV. USE CASES FOR ENCRYPTION

Data Protection: Ensures that sensitive data like passwords, credit card numbers, and personal information are securely stored or transmitted.

Communication Security: Used in securing communications like emails, instant messaging, and voice over IP (VoIP).

Digital Signatures: Verifies the identity of the sender and ensures the integrity of the message.

Secure Online Transactions: Encrypts payment details during online purchases to protect users from fraud.

Encryption is a crucial component in modern cyber security, providing a fundamental defense mechanism against data breaches and unauthorized access. Different algorithms are chosen based on the trade-off between security, performance, and ease of key management.

Summary Comparison Table:

Feature	Blowfish	AES	DES
Key Size	32–448 bits	128, 192, or 256 bits	56 bits
Block Size	64 bits	128 bits	64 bits

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 77-82 DOI: https://doi.org/10.63671/ijsssr.v4i1.493
Volume: 4 | Issue: 1
April-June 2026

Feature	Blowfish	AES	DES
Rounds	16	10 (128-bit), 12 (192-bit), 14 (256-bit)	16 rounds
Speed	Fast (especially for small data)	Fast (especially for larger data)	Fast, but outdated and insecure
Security	Secure but 64-bit block size is a limitation	Very secure, resistant to attacks	Insecure due to small key size
Primary Use Cases	File encryption, legacy systems	Modern encryption for web, government, and enterprise	Legacy systems (now obsolete)
Vulnerabilities	Potential birthday attacks due to 64-bit blocks	None found for standard key sizes	Vulnerable to brute-force attacks

- AES is the modern standard and is recommended for all new projects due to its strong security, efficiency, and wide adoption.
- Blowfish was once popular but is less secure now because of its 64-bit block size. It is still useful in some legacy applications but is being replaced by AES.
- DES is now obsolete due to its small key size and vulnerabilities to brute-force attacks. It's no longer safe for use in any modern cryptographic system.

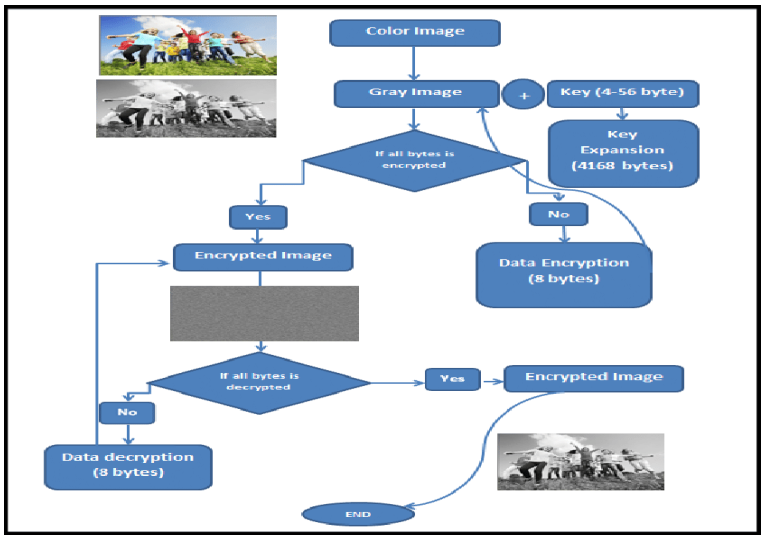
IV. METHODOLOGY

Settle on the right symmetric encryption algorithm depends on various assorted factors such as encryption/decryption speed, key size, security, efficiency, and compatibility with the devices and software being used [16]. Besides, the choice of symmetric encryption algorithm also depends on the type of data that is being encrypted and the level of security required. For instance, if security is a top priority, then algorithms such as AES or Two-fish might be more suitable, while for cultivate encryption and decryption, algorithms such as Blow fish may be considered as a better option. It is must to weigh the trade offs between security and productivity when choosing a symmetric encryption algorithm [17].

V. IMPLEMENTATION

The implementation of the Blow-fish algorithm in C# using Visual Studio 2012 on Windows 8 involves using a 128-bit encryption key, either loaded from a file or generated, to generate the P-box and S-box arrays. The input message is encrypted using ECB mode of Blow-fish encryption and divided into 64-bit data blocks which are encrypted with a specified number of rounds [18]. The decoding phase involves inverse wavelet transform on the stego image, extracting a bit stream, and using the decryption module of Blow-fish to get the input plain text [19]. Figure Embedded model showing compressed, blurred and colour image and Gray image.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 77-82 DOI: https://doi.org/10.63671/ijsssr.v4i1.493
Volume: 4 | Issue: 1
April-June 2026



Visual of blow-fish algorithm process

encrypted images in steps to propose secured model and add the new image to the database Embedded model using increase the key size its yes means it go the encryption image.its condition is no the the data in-encryption size are going to increase the key size. The image is ready to increase the bytes the image is going to gray image,its going to end.blurred and encrypted to propose secured system model for revealing the secured image.

V. CONCLUSION

In this paper, we explained about the use of an encryption algorithm while storing or retrieving information on the cloud. Blow-fish encryption algorithm is one of the fastest encryption algorithms. Blow -fish is a very efficient data encryption algorithm. It creates 64-bit keys, which are extremely efficient. Huffman coding is a technique used in the blow-fish algorithm to compress data.By employing these encryption approaches, we can encrypt data safely and effectively while also lowering the device's battery consumption. We can improve decryption algorithms and non-repudiation in the future. It is possible to improve authentication by increasing the key size.

REFERENCES

1. B. Joshi, Karuna P, Theofanos, Mary, And Stanton, ―Framework for Cloud Usability NIST Special Publication 500-316 Framework for Cloud Usability,‖ pp. 1–18, 2015
2. Raptis A., Perdikis C. and Takhar H. S., “Effect of thermal radiation on MHD flow”, Appl. Math. Comput.,153,
3. Cowling T. G., “Magnetohydrodynamics, Inter Science Publishers”. New York, 1957.
4. T. Ramaporkalai,―Security Algorithms in Cloud Computing SECURITY ISSUES OF CLOUD,‖ vol. 5, no. 2, pp. 500–503, 2017.
5. R. Ahmed and M. L. Ali, ―Minimization of Security Issues in Cloud Computing,‖ 2017.
6. C. Paper and K. P. Siemens, ―Cloud computing security issues and challenges,‖ no. June 2010.
7. R. Kaur and R. P. Singh, ―Enhanced cloud computing security and integrity verification via novel encryption techniques,‖ Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014, pp. 1227–1233, 2014.
8. M. Shashi, ―Cloud Computing Models : Background, Data security, & Security Issues,‖ vol. 2, no. 2, pp. 1–6, 2017.
9. H. Kaur, ―A Novel Technique of Data Security in Cloud Computing based on Blowfish with the MD5 method,‖ vol. 3, no. 6, pp. 828–837, 2017.
10. A. Pansotra and S. P. Singh, ―Cloud security algorithms,‖ Int. J. Secur. Its Appl., vol. 9, no. 10, pp. 353–360, 2020.