WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Survey on AI Based Data Privacy System for Cloud File Sharing

***Gayathri Devi R[1], Subalakshmi R[2], Keerthika T[3], Praveenkumar P[4]`***

[1,2,3,4]Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India

**ABSTRACT –**

In our information society, which is characterized by a growing variety of enabling and supporting technologies and services, privacy is one of the most significant social and political issues. The cloud software is one of these. We formalize Blowfish-based cryptography in this effort. Create a protocol that permits verifiable file search for enterprise-scale cloud storage applications using the verifiable file search issue. Consider a company with many employees that wishes to transfer company data files to a cloud storage company. The employee submits the file name to the cloud and asks for the right file to be returned later to retrieve the file. The cloud may deceive users by claiming that files already present do not exist or that files that do exist do not exist for a variety of reasons (economic incentives, active insider/outsider assaults, etc.).

**Key points**: Data privacy, Data De-identification, Blowfish algorithm.

## 1. INTRODUCTION:

***Advanced Encryption Standard (AES) -***

BLOWFISH CIPHER - Advanced Encryption Standard is referred to as BLOWFISH. Data Encryption Standard is replaced by the Blowfish key encryption technique in use today (DES). In November 2001, NIST chose Blowfish as a Federal Information Processing Standard because it offers robust cryptography (FIPS-197). Three key sizes are used by the Blowfish algorithm: encryption keys of 128 bits, 192 bits, or 256 bits. Increases in key size result in both an increase in the number of bits needed to encrypt the data and an increase in the complexity of the encryption method since each encryption key size has a slightly different effect on how the algorithm functions.

The Two of the Belgian cryptographers, Vincent Rijmen and Joan Daemen, are the creators of blowfish. The encryption algorithm BLOWFISH is used (and reverse decryption). a process is a collection of stages that are followed with clarity. The source of the information is plain text, and the encrypted form as cipher text .

The Blowfish algorithm is a Blowfish block cypher that has the ability to both encrypt and decode data. Data is encrypted into cypher text, an incomprehensible form; this cypher text is then decrypted to restore the original plain text version of the data. It can be used to safeguard digital data by making the code unreadable.

**Blowfish -** Data is encrypted and decrypted using just one key with BLOWFISH keys encryption. The key needs to be shared before being transmitted between entities. Keys are crucial because anyone can decrypt data if a weak key is used in the technique. The size of the employed key affects the strength of Blowfish key encryption. Longer keys used in encryption for the same technique are more difficult to crack than shorter keys. Strong and weak keys for encryption techniques like RC2, DES, 3DES, RC6, Blowfish, and BLOWFISH are numerous. One 64-bit key is used by RC2 and DES.

Whereas BLOWFISH utilizes a variety of (128,192,256) bits keys, Triple DES (3DES) uses three 64-bit keys. Blowfish employs a number of (32-448) keys. RC6 employs a variety of (128,192,256) bit keys, and where default is 128 bits [1-3].

Blowfish key encryption - Problems with key distribution are resolved with it. His two keys—a private key and a public key—are used by the BLOWFISH key. The private key is used for decryption, while the public key is used for encryption (e.g. RSA and digital signatures).

While the private key is solely known to you, the public key is accessible to everyone. No distribution is required prior to mailing. Public-key encryption is computationally expensive, depending on mathematical operations, and not very effective for small mobile devices like cell phones and PDAs.

The occasionally be compelled to sign legal, business, or other documents. The use of both private and public key algorithms has led to the development of numerous digital signature techniques. Blowfish key for Public Key - As an alternative to RSA which is BLOWFISH Key algorithm, there are two keys. One must be private key. The system is also used to sign a message digitally. Rivest- Shamir-Adleman (RSA) is widely used BLOWFISH key algorithm for decrease elliptic curve cryptography.

**Cipher Text** - This is the encrypted message produced by applying the algorithm to the plaintext message using the secret key.

**Block Cipher** - Block cipher is a type of the BLOWFISH-key encryption algorithm that transforms a fixed-length block of plaintext data into block of cipher text data of the same length.

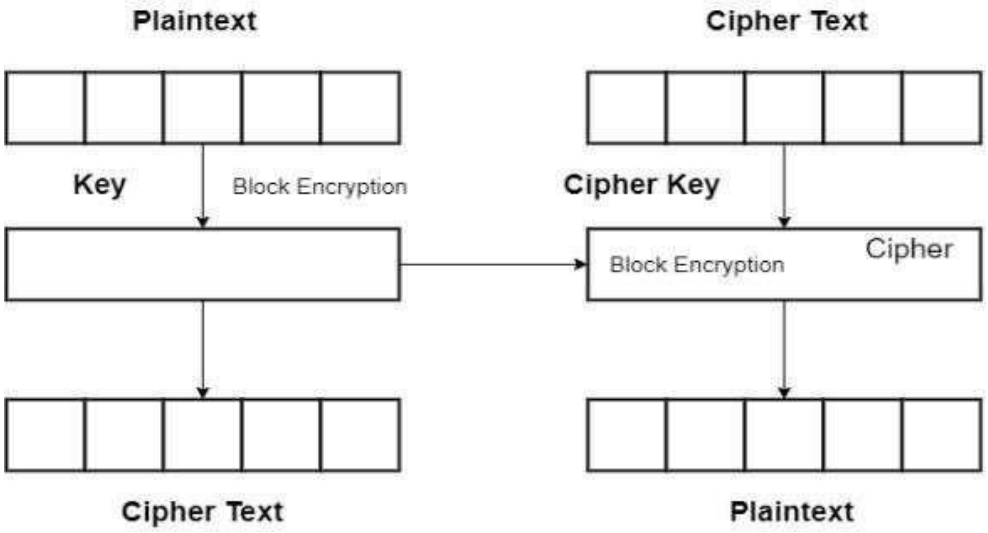


*Fig 2.3 Block Cipher*

**The Blowfish Cipher:**

| Key size(word/byte/bits) | 4/16/192 | 6/24/192 | 8/32/256 |
|---|---|---|---|
| Number of rounds | 10 | 12 | 14 |
| Expanded key size(words/byte) | 44/176 | 52/208 | 60/240 |

Representation of key size, number of rounds, expanded key size The key size can be independently specified to 128,19 or 256 bits.

The development of a suitable, economical security system is the goal of this project. The MAC address and cloud are two essential components of this project's security. Here, the private key is the one that is used. Under the control of a private key that the user has provided, this conversion is carried out. Using the same private key, decryption is accomplished by performing the inverse transform on the encrypted text block. In many block cyphers, the fixed length is referred to as the block size. As processor technology advances, the block size rises to 128, 192, or 256 bits. The block cypher conversion is shown in the diagram below. Block cyphers include DES, Triple-DES, and Blowfish, among others.

Various plaintext blocks map to Block cyphers effectively provide a permutation of the set of all possible messages since distinct blocks of plaintext map to different blocks of cypher text (to allow for unique decoding). Since it is a function of the secret, the permutation carried out during every given encryption is a secret. And both encryption and decryption are performed using block cypher.

Here, a phone and computer are both used. The maximum block size for 128 bit cryptosystems is 128 bits. The application runs on the computer, which is the server side, and the phone, which is the client side, is used to authenticate approved devices. to safeguard the file against a cryptosystem. Data must be encrypted or decrypted using this BLOWFISH key.

To increase the security of the file, data encryption is done using cryptographic keys. The data must be decrypted using the same key. As a result, we must either memorize the key or put it away. We must store information since memorizing it is impractical and we must be able to access it in order to decrypt the data back into its original, meaningful form when no one else can. The cryptographic keys are used in data encryption to make the file more

secure. The same key must be used to decrypt the data. This means that we have to either memorize the key or store it somewhere. Memorizing it isn't practical, so we must store it so that we can recall it when we want to decrypt the data back into its meaningful form, but no one else can.

## LITERATURE SURVEY:

**1. Research of Data Encryption Algorithm Based on S-DES -** This paper mainly studies one kind of simple Data encryption algorithm which can help general users to keep secret from the data information. The algorithm is modified from the DES whose processing may be divided into three steps: initial transform IP, 16 round iterations, and initial inversed transforms IP-1. Initial transformation and inverse transformation can enhance difficulty to be understood for data, and not to affect security of data. Modified encrypted algorithm, namely S- DES, carries on two round iterative encryptions to clear text. The length of block and secret key reduced. Therefore S- DES algorithm is more inexpensive than the DES encryption algorithm and remains many merits of DES. Objectives: a) Secure Data encryption using SDES b) Using simple 2 rounds to make it less complicated.

**2.Data encryption algorithm based on chaotic map and S-DES -** Due to the initial sensitivity of chaos card, its application is becoming more and more popular. Data encryption algorithms based on chaos theory are a hot research area these days. Disruption and proliferation are the methods required to achieve data encryption. However, the chaos map's initial sensitivity and randomness can be used to achieve the chaos and diffusion objectives. The S-DES system can encrypt the incoming binary data flow, but it is risky due to the fixed system structure and few keys. However, the initial sensitivity of this chaotic Lu map can be successfully applied to the system of SDES, yielding S-DES with larger random sets and key sets.

A dual data encryption algorithm based on S-DES and Lu card is proposed. Compared to conventional methods, it has advantages such as easy-to-understand, fast encryption speed, large key size, and sensitivity to initial values. Objectives: a) Using chaotic map to make SDES more secure b) Increasing encryption speed c) Making it easy to understand.

**3.Digital Data encryption algorithm based on chaos and improved DES -** In recent years, encryption technology has been developed quickly and many Data encryption methods have been put forward. Chaos based Data encryption technique is a new encryption technique for Data.

It utilizes chaos random sequence to encrypt Data, which is an efficient way to deal with the intractable problem of fast and highly secure Data encryption. However, the Chaos based Data encryption technique has some deficiencies, such as the limited accuracy problem. This paper researches on the chaotic encryption, DES encryption and a combination of Data encryption algorithm, and simulate these algorithms, through analysis of the algorithm to find the gaps. And on this basis, the algorithm has been improved.

The new encryption scheme realizes the digital Data encryption through the chaos and improving DES. Firstly, new encryption scheme uses the Logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the Data chaotically, then makes double time encryptions with improvement DES, displays they respective merit. Theoretical analysis and the simulation indicate that this plan has the high starting value sensitivity, and enjoys high security and the encryption speed.

The new encryption scheme realizes the digital Data encryption through the chaos and improving DES. Firstly, new encryption scheme uses the Logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the Data chaotically, then makes double time encryptions with improvement DES, displays they respective merit. Theoretical analysis and the simulation indicate that this plan has the high starting value sensitivity, and enjoys high security and the encryption speed.

**4. Blowfish cryptography in color Data steganography by genetic algorithms ---** This work includes the BLOWFISH encryption algorithm, which improves the security of hidden data with two steganographic methods: genetic algorithms and path relinking. We also combine them to propose a new hybrid approach that goes beyond the LSB (least significant bit) replacement technique presented in the works cited in the Steg data quality literature. The ability to hide data with color data is greatly improved, giving him more than three times more space available for information compared to the usual steganographic approach used with grayscale data. Additionally, all kinds of digital information can be hidden in cover data, from text and compressed files to executable programs. this considerably increases the scope of application of the technique for transmitting information inside a typical Data, hiding the data from intruders. Objectives: a) Using BLOWFISH to secure Data b) Changing LSB to use steganography

**5. A Modified MD5 Algorithm Incorporating Hirose Compression Function -** Hashing is a widely used method in cryptographic protocols and data integrity verification. Among the most commonly used cryptographic hash functions is MD5 for various applications. However, MD5's strength against brute force attacks comes from its algorithms that address security holes and vulnerabilities. In this study, we present a round-function modification of MD5 with an innovation to incorporate the Hirose function. Simulations of the proposed algorithm were done in PHP.

Test results showed that the modified MD5 algorithm produced a more secure hash output. Through several tests such as the avalanche test and the differential attack test,

The simulation results showed the superiority of the modified algorithm over the typical one. To prove the concept, the research used an inverted 17th bit. An avalanche effect test of normal MD5 and modified MD5 results in a Hamming distance of 58.38 for the former, which is 42.71%.

## CONCLUSION:

The main advantage with the Advanced Encryption Standard is to maintain the secret communication between the Encryption and Decryption. It is the Blowfish key encryption algorithm. This reduces the complexity of the Encrypt and Decrypt the data. Cipher key is same for both the Encryption and Decryption process ASP.NET code is used to develop the implementation of Encryption and Decryption process. Each program is tested with the some of the sample vectors provided by results are perfect with minimal delay. In the case of 192,256-bit key algorithm, it requires 192,256-bit plain text and 128-bit cipher key.

Even the Blowfish -128 bit offers a sufficiently large number of possible keys, making an exhaustive search impractical for many decades, provided no tech breakthrough cause computational power available to increase dramatically and that theoretical research does not find a short cut to implemented and keys are generated. It is necessary to ensure each and every implementations security, an important correctly implemented BLOWFISH-128 is likely to protect against a million and against individual budgets for at least another ten years.

**REFERENCES:**

[1] FIPS 197,"Advanced Encryption Standard (BLOWFISH)", November 26,2021.http://csrc.nist.gov/publication/fips/fips197/ fips-197.pdf.

[2] J.Daeman and V.Rijmen Blowfish Proposal: Blowfish Algorithm Submission September 3,2019.

[3] FPGA simulation of round 2 "Advanced Encryption Standards" http://csrc.nist.gov/CryptoToolkit/Blowgish.

[4 Tilborg, Henk C. A. van. "Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial".

[5] Peter J. Ashenden, "The student's Guide to VHDL", 2nd Edition, San Francisco, CA, Morgan Kaufmann,2020 understanding mix columns.

[6] William Stalling (2019), Chapter 4.6 Finite Fields of the Form GF(2n) – Multiplication, in Cryptography and Network Security.

[7] KitChoy Xintong (2021) Understanding the Blowfish Mix-Column Transformation calculation.

[8] J. Daemen and V. Rijmen, The block cipher Blowfish, Smart Card research and Applications, LNCS 2020, Springer- Verlag,-pp. 288-296.

[9] Dhiman Saha, Debdeep Mukhopadhyay,Dipanwita Roy Chowdhury (PDF). Diagonal Fault Attack on the Advanced Encryption Standard from the original Archived from on 22 December 2019.

[10] J. Nechvatal, ET. al., Report on the Development of the Advanced Encryption Standard (BLOWFISH), National Institute of Standards and Technology, October 2, 2020.

[11] "NIST.gov - Computer Security Division - Computer Security Resource Center". Csrc.nist.gov. Retrieved 2019- 12-23.

[12] AndreyBogdanov, Dmitry Khovratovich, and Christian Rechberger (2021). "Biclique Cryptanalysis of the Full BLOWFISH".