International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST52310245

# Effectual Cryptography Approaches for Cloud Storage Image Encryption

**Mamta Khanchandani*[1], Dr. Sanjay Buch[2]**
*[1]Research Scholar, Bhagwan Mahavir University, Surat, Gujarat, India
[2]Dean, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

ARTICLEINFO

**Article History:**

Accepted: 05 March 2023
Published: 22 March 2023

**Publication Issue**
Volume 10, Issue 2
March-April-2023

**Page Number**
281-294

ABSTRACT

In recent years and with the great progress of the use of cloud computing and their uses that covered most aspects of modern life as well as provide a variety of services, such as the formation of computing resources, cost control, sustainability, mobility and service flexibility. However, there are challenges to cloud computing, the most important of which is data security and transmission. Cryptographic is the science of protecting data by converting data (plain text) into an incomprehensible format (cipher text) for unauthorized individuals through the use of mathematical techniques. This paper provides work for the most common encryption algorithms that are utilized to encryption of data in cloud computing and presented some of papers that based on the most common cryptographic techniques such as DES, 3DES, Blowfish, AES, RSA, D-H, ECC and others. This way paves the way for finding the suitable encryption algorithm to protect the data in the cloud environment. The AES outperforms the other algorithms in term of encryption time.

**Keywords :** Cloud Computing, Cryptography, Symmetric, Asymmetric, Data Security

## I. INTRODUCTION

Cloud computing has become a general concept and it is used daily. It is a model which offers variety of services and in different areas, in health, industry, agriculture, and military fields and among others fields. Our use of social media and sends documents, photo and posts is only a simple example of cloud computing. It is widely used in the recent years because of its easy access like the use on demand and scalability [1]. The National Institute of Standards and Technology (NIST) is formally defined a cloud computing in [2]. The cloud computing provides different services; these services put forward three models (i)Software as Service (SaaS): In this type of cloud service, the use cannot manage the component, services, memory and operating system in the cloud network. There are partial settings that can be managed by the user [3] (ii) Platform as service (PaaS): enables users to build many applications using

different programming languages. These applications can be created by various services, tools and libraries that are supported by service provider. For example, Python language is one of programming language to build applications in Google App engine. (iii)Infrastructure as service (IaaS): This type considers the core engine for the cloud virtually. It is included the virtual servers, limited storage and processing capacity. The user can control the operating systems, storage resources, network and applications installed on this platform. It is clearly shown that Simple Storage Service (S3) in the Amazon, all users can access and store their data using a web service interface. Amazon's Elastic Compute Cloud (EC2) is a well IaaS platform that the clients create and configure the virtual machines. All the service models have the fundamental characteristics of cloud computing: On demand self- service, broad network access, resource pooling, rapid elasticity and measured services [4]. NIST summarized the cloud deployments models which can be either internally or externally implemented, as follows: Public, private, hybrid, and community depending on company policies in term of cost and sharing [5]. Public cloud is used to share resources for general public purpose "pay-as-you-go". It may be managed and controlled by the government organization. The users are not aware of the users that sharing the cloud. Community cloud may be managed and controlled by a group of users in companies to share policies and security requirements. Private cloud is established to serve one company or organization. Hybrid cloud results from one or more cloud (private, community, and public). Figure 1 shows cloud computing service and model.

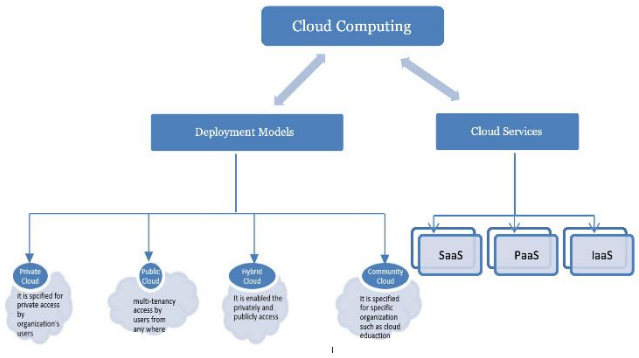


**Figure 1.** Cloud computing services and model

Data security has been always the main concern about cloud computing services cryptography is a main trend to achieve data security. Since the introduction of cloud computing technology, several cryptography solutions have been proposed for protecting outsourced data and user privacy and for ensuring that this data are not going to be leaked to unauthorized third party. Most of these solution schemes aim at achieving a trade-off between security and functionality. This paper implements cloud-based image encryption using common cryptographic techniques and also comparative for the most common cryptographic algorithms in term of encryption time. The rest of the paper has been organized as follows: Section 2 presents a definition about cloud computing security. In Section 3, we describe the method of cryptography techniques. Section 4 discusses and compares some of papers that are based on the most common cryptographic techniques and also compare the most common cryptographic algorithms. Section 5 discusses the application of securing image in cloud computing. Finally, conclusions will be presented in section 6.

## II. CLOUD COMPUTING SECURITY

With the increased use of the Internet that is widely spread in our world, and with the advent of cloud computing technology in recent years, interest in cloud technology is increased and becomes widely used in various fields, so security of this technology becomes necessary. Data protection is a very

important issue especially in cloud computing because most service providers do not usually have a robust security system to protect data centres, so it is necessary to rely entirely on the lessor to process its basic environment to maintain its data safely [6]. It is mandatory for the organization and multi tenancy to use a suitable data encryption algorithm through cloud computing. Each of encryption algorithms has advantages and disadvantages in term of many security metrics such as throughput, entropy, encryption and decryption time and memory usage and avalanche effect [7].

## III. CRYPTOGRAPHY ALGORITHMS IN CLOUD COMPUTING

Cryptography is the science based on maintaining the confidentiality of data by converting it to the unreadable form by certain algorithms. It is utilizing science of mathematics for converting plaintext data (P) into format of an ambiguous ciphertext (C), this process is known as "Encryption", with using one or more of encryption algorithms (E). While the process of returning the ciphertext back to plaintext known as "Decryption", with using one or more of decryption algorithms (D). For encryption and decryption utilizing encryption keys (k1and /or K2). Figure 2 shown encryption and decryption process. Figure 3 shows the main classification of cipher types in general.

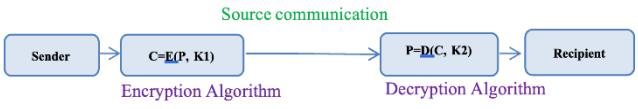


**Figure 2.** Encryption and decryption process

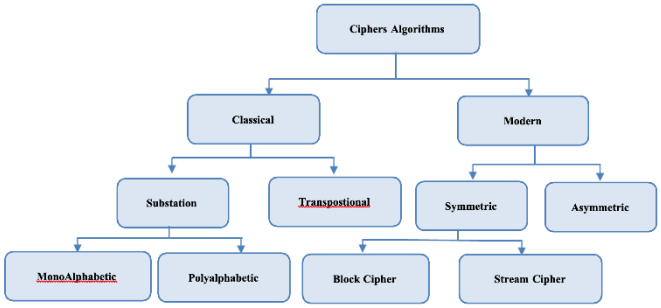


**Figure 3.** Classification of cipher algorithms

Cryptography algorithms are classified according to the encryption key used. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, hybrid algorithms and Hashing algorithms. In symmetric key algorithm, process of encryption and decryption of the data utilize one key called private key. While in asymmetric key algorithm cryptographic two keys are used, private key (used for decrypting data) and public key (used for encrypting data). In hashing algorithms, data will compress for signing to standard fixed size. Whereas in hybrid encryption two or more algorithms of the same type or more than one type are used. Hybrid encryption is considered a very high level of safety due to the difficulty of decoding to use more than one algorithm for data encryption.

### 3.1 Symmetric-key encryption

Symmetric-key encryption (also known as secret-key encryption) is one of the simplest types of encryptions that use the same key for encryption and decryption. This key is known to both the sender and receiver as shown in Figure 4 symmetric-Key encryption utilizes secret-key that can be a number or a message of random letters [8].

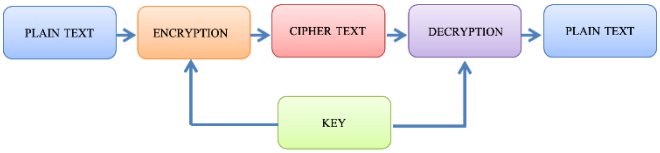


**Figure 4.** Symmetric encryption

Symmetric algorithms can be categorized into one of two main used methods for encryption techniques

that are based on the form of the input data they operate on, either block cipher or stream cipher. The main distinction between block and stream cipher is that block cipher takes a data and break it into a fixed size of blocks and converts one block at a time [9][10].
Block cipher encryption: In this method cryptography, the encrypted and decrypted of data is formed as block of data (a fixed size of n-bits of data) at one time. The plaintext is divided into blocks which are then fed into the cipher system to produce blocks of ciphertext. There are a lot of popular algorithms that operate according to the block cipher such as Data Encryption Standard (DES), Advanced Encryption Standard AES, Triple Data Encryption Standard (3DES) and Blowfish.

Stream cipher encryption: In this method cryptography, data is encrypted and decrypted in term of bit of data (a fixed size of one bit of data) at one time. Stream cipher comprises of two main parts: the first part is a key stream generator which the main unit in stream cipher encryption technique. While the second part is a mixing function which is just an XOR functions. The most popular algorithms that build on Symmetric-Key encryption are: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Blowfish (BF), etc.

### 3.2. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard is considered as the first of the most famous symmetric cryptography algorithms. It is proposed by the National Institute of Standards and Technology (NIST) in the 1970 and published as an official Federal Information Processing Standard (FIPS) in 1977 [11][12]. DES considers the first encryption algorithm developed based on the concept of the Feistel Structure. It is designed to cipher block of data with 64 bits for each block. The encryption key length uses 64 bits for encryption and decryption as standard but only 56 bits are used and discard 8 bits. The generated key (56 bits) will divide into two halves, each half with 28 bits. The permutation and expansion processes will be used to generate 48-plaint text and 480bits key length from the right halve. The latter will be XORed and substituted into 32-bits plaintext by S-Box. Final 32-bit plaintext value passes from permutation P-box and XOR with left halves of 32-bit plaintext. This process will do till 16 rounds and 48-bit key value will be changed at each round. DES is flexible because it works in Output FeedBack (OFB) and Cipher Block Chaining (CBC). Figure 5 shows encryption in Data Encryption Standard algorithm.

It is noticeable in the DES algorithm that in the case of a simple change in the plain text it generates a major change in the cipher text as well that each section of the cipher text depends on many sections of the plaintext and this makes the cipher in the algorithm strong [8], so DES is still widely used for data protection. This does not mean that there are disadvantages in the algorithm, one of which is the short length of the key.

#### 3.2.1. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard is one of the most important and most popular algorithms for encryption. In December 2001, National Institute of Standards and Technology (NIST) published Advanced Encryption Standard as FIPS-197 in the Federal Register [13]. The main goal of its development is to replace DES algorithm after many attacks recorded the weaknesses of DES, which make it an insecure block cipher. AES is a block cipher. It encrypt blocks of plaintext, each block Contains of 128bits and using different value of key 128 bit(16 byte), 192 bit (24 byte) or 256 bit (32 byte) depending on the number of rounds 10, 12 or 14 rounds. Advanced Encryption Standard algorithm authorizes a 128 bit data (plain text) length, and divides into four blocks. These blocks are patronize as array of bytes and organized as a matrix of the order of 4×4 that is called the state. To increase the protection in encryption, for each 128-bit

plain text (block) AES uses four types of transformations in each round. These transformations are [14]:

**1. Substitution bytes (SubBytes):** data block in Advanced Encryption Standard algorithm consists 128 bit; this means that each block of data contains 16 bytes. In subbyte transformation, each 8-bit (Byte) in a block of data transforms into another block using an 8-bit (Byte) substitution box which is called as Rijndael S-box. Figure 6 shown substitution bytes transformation.

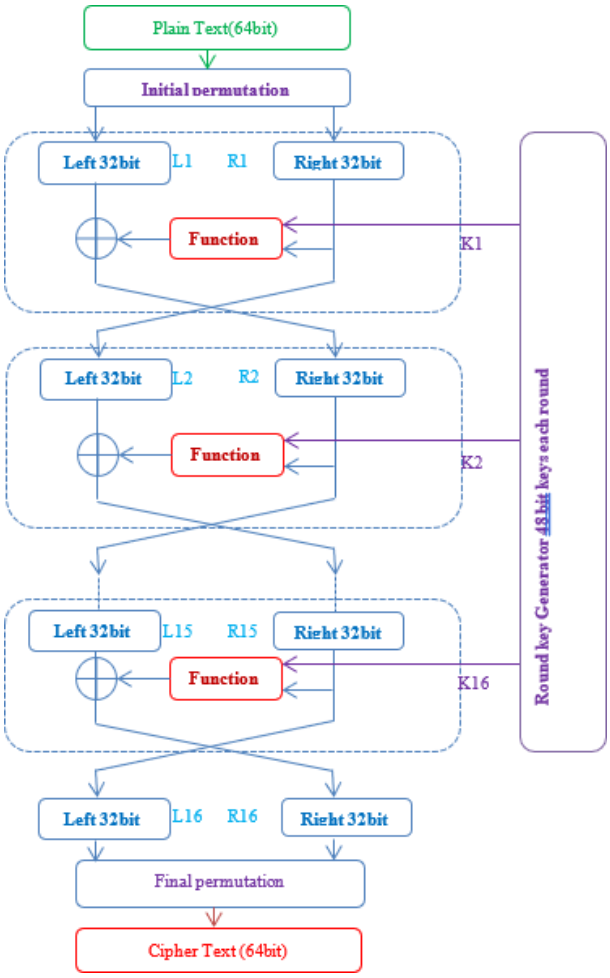


**Figure 5.** Encryption in data encryption standard algorithm

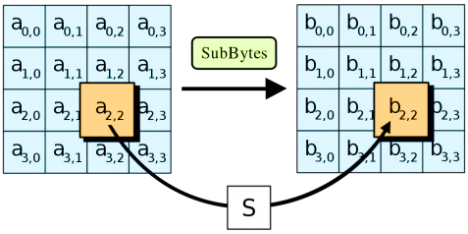


**Figure 6.** Substitution bytes transformation [15]

2. Permutation (Shift Rows): Each of the four rows of the matrix is rotated to the left. This rotation is as follows:

- The 1st row is not shifted.
- The 2nd row is shifted one (byte) place into the left.
- The 3rd row is shifted two (byte) places into the left.
- The 4th row is shifted three (byte) places into the left.

After this process the outcome is a matrix consisting of 16 bytes. Figure 7 shows shifted rows transformation.

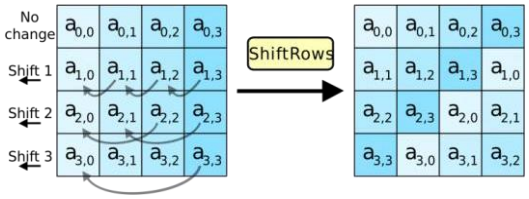


**Figure 7.** Shifted rows transformation [15]

3. MixCloumns: This process is a simple substitution one. Each column of matrix is transformed using a matrix multiplication by using (finite GaloisField-GF(28)). After this process, the outcome will be a matrix consisting new matrix contains sixteen new bytes. Figure 8 showed mixed columns transformation.

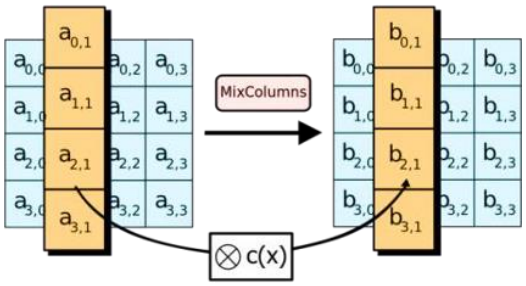


**Figure 8.** Mixed columns transformation [15]

4. AddRoundKey: Here, the XOR process operates among state and round key matrix, as shown in Figure 9. These four stages are repeated in each round which their number 10, 12, or 14, depending on the size of

the key 128, 192, and 256 bits. Figure 10 shows Advanced Encryption Standard encryption algorithm.

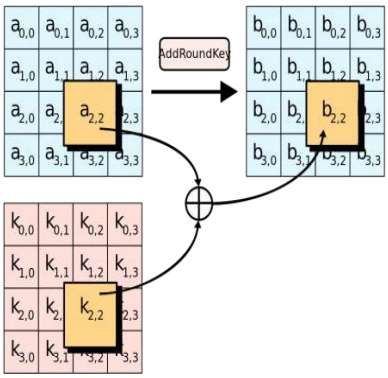


**Figure 9.** Adding round key [15]

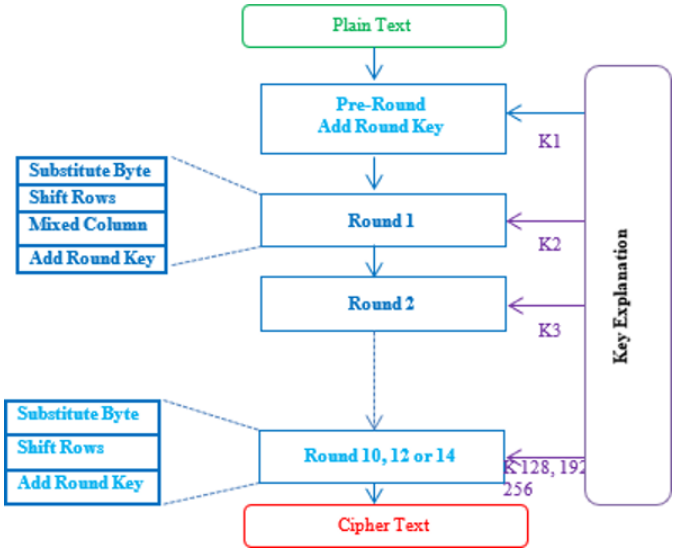


**Figure 10.** Encryption in advanced encryption standard

Advanced Encryption Standard algorithm has proven its strength and high security against brute-force attacks due to it is desired multi bit key to encrypt the information, this is one of its advantages. In a decryption algorithm, the same sequence of encryption process will be followed but with reverse each transformation step.

### 3.1.2 TRIPLE DATA ENCRYPTION STANDARD (3DES)

Because of the defects in the data encryption standard algorithm where a short-key used (56-bit) which is not secure enough to encode important data and sensitive data, so IBM has in 1998-1999 developed Triple Data Encryption Algorithm (TDEA). 3DES operates in three phases: first phase encryption of DES is used, second phase decryption of DES is used, and third phase encryption of DES is used. It functions by using three keys (k1, k2, k3) each key is 64 bit length, where the plain text is encrypted by first phase with K1, then decrypted by second phase with K2, and also encrypted by third phase with K3 [16]. See Figure 11. The encryption process can be expressed as C = E (D (E (P, K1), K2), K3). Decryption process can be interpreted as P = D (E (D(C, K3), K2), K1).

### 3.2.3. BLOWFISH (BF)

In 1993 Bruce Schneider developed algorithm called Blowfish algorithm. Bruce Schneider considered this algorithm a successor to DES algorithm [17]. It is Feistel Structured algorithm and has block cipher uses 64- bit of data with 16 round and the key length is fluctuating from 32 bits and can be as long as 448 bits. The BF algorithm contains mainly two phases: data encryption phase and key expansion phase. Blowfish uses a large number of subkeys which are constructed during the Key expansion phase. This phase converts a variable- length key which in common 56 bytes (448 bits) into an array of sub-keys called P-array consists of eighteen 32-bit sub-keys totaling 4168 bytes. There are also four 32-bit S-boxes. The keys must be computed before any data encryption or decryption [18]. The creation of sub-keys further increases security, because a hacker would have to crack more than just the original key.

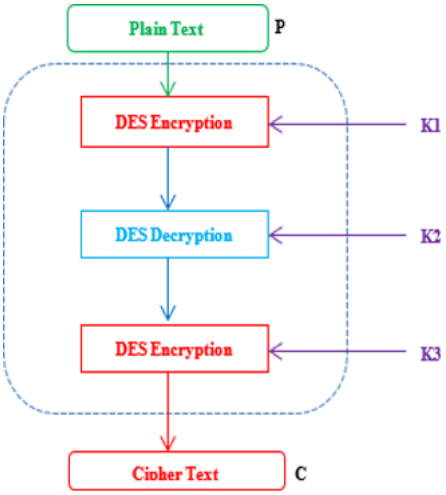


**Figure 11.** Encryption in triple data encryption standard algorithm

The second part of the Blowfish routine that is a data encryption is done through 16 Fiestel network rounds, a swap operation and two exclusive-or operations. The F function takes the 32-bit input and divides it into 4 bytes (8-bits each). These four values are then used for table lookup in their corresponding S-Boxes. A graphic representation of Blowfish is given in Figure 12.

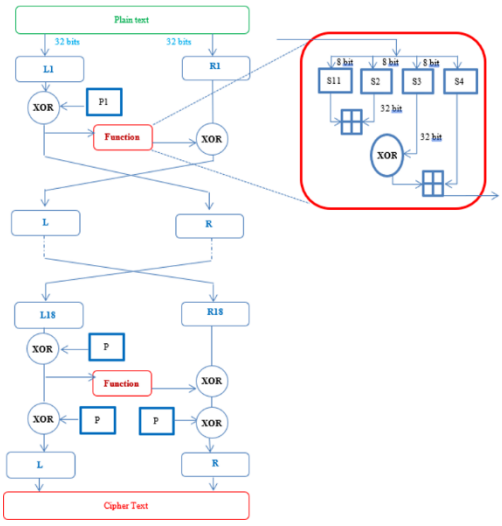


**Figure 12.** Encryption in blowfish algorithm

### 3.3 ASYMMETRIC ENCRYPTION

It is known as a public key encryption which private and public keys are used. Asymmetric encryption uses one key (public key) for encryption while uses another key (private key) for decryption. The public key may be freely distributed, while its paired private key must remain secret. Figure 13 shows asymmetric encryption. The most popular algorithms that build on this type of encryption are Rivest, Shamir, & Adleman (RSA), Diffi-Hillman(DH), Elliptic Curve Cryptography (ECC), etc.

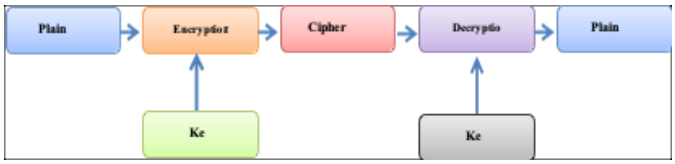


**Figure 13.** Asymmetric encryption

#### 3.3.1 RIVEST-SHAMIR-ADLEMAN (RSA)

In 1977 Ron Rivest, Adi Shamir, and Leonard Adleman developed algorithm named after their names (RSA). RSA is an asymmetric encryption algorithm so it uses two keys, one to encrypt messages with a public key (known to all) and the second to decrypt using a private key (secret, known to the user only). To encrypt a Message (plaintext) using public key that can only be decrypted using private key. In RSA cannot use the same key for both the encryption and decryption of the message. RSA algorithm consists of three phases: Key Generation phase, encryption phase, and decryption phase.

#### 3.3.2 DIFFIE-HELLMAN ALGORITHM (DH)

Whitfield Diffie and Martin Hellman developed the first public-key algorithm constructed in 1976. This algorithm is used for exchanging cryptography keys between two users [19]. It is used for key exchange algorithm, by first institution a shared key (private key) to use for the inter communication. The shared private key can then be utilized to safely exchange a cryptographic encryption key. That key then encrypts traffic between the two systems.

#### 3.3.3 ELLIPTIC CURVE CRYPTOGRAPHY (ECC):

In 1985, Koblitz and Miller developed Elliptical curve cryptography (ECC). It is considered one of the public- key encryption algorithms. The process of generating cryptography keys is based on the elliptic curve theory, so ECC uses the properties of this

theory to generate keys. For the decryption process, it uses the private key while the encryption process uses the public key. ECC uses a 164-bit key and achieves a high level of security, while other technologies require a 1024-bit key to achieve this.

### 3.4 HASHING ENCRYPTION

It is one of the cryptography algorithms to hash the plain text without key. It is used a hash function to convert the plain text into series of random characteristics with a fixed sized of length. It is a mathematical algorithm that maps data of arbitrary size to a hash value of a fixed size called message digest (one way function). With a message digest, it is hopeless to get back or find the authentic string. However, in recent years several hashing algorithms have been compromised as happened to MD5. Hash values can be created for different data, meaning that is easier comparing hashes than the data itself. Some examples of hashing algorithms are: Message Digest (MD5), Secure Hash Algorithm (SHA) Figure 14 shows Encryption in hashing algorithm.


**Figure 14 Encryption in hashing algorithm**

#### 3.4.1 MESSAGE-DIGEST ALGORITHM 5 (MD5)

In 1991, Ron Rivest developed Message digest 5 or MD5 which is considered as one of hashing (message-digest) algorithm. This algorithm takes input data of any length and outputs to be digestible with a fixed length of 128 bits The MD algorithm uses a 512-bit block size that will be manipulated and produced 16 subblocks, each subblock is 32 bits. The MD5 algorithm is developed to replace its predecessor MD4.

### 3.5 HYBRID ENCRYPTION

In this type of encryption, more than one algorithm for encryption can be merges. This type of encryption can merges algorithms of the same type or more than one different type (symmetric-key, asymmetric-key or hashing).This combined encryption gives the possibility to take advantage of the strengths of each form of encryption. Hybrid encryption is considered a very high level of safety due to the difficulty of decoding to use more than one algorithm for data encryption[20][21].

## IV. ANALYSIS OF CRYPTOGRAPHY ALGORITHMS

This section will discuss the most important algorithms used in data encryption in the cloud computing and present their capabilities in data encryption and reviews the structure of the algorithm. The structure is characterized by a set of variables such as the block size, key size, and number of rounds. In the end, these are the factors which affect the security of an algorithm. The size of the key in the algorithm plays an important role in its security, the larger the size of the key, the higher the security when other factors are considered to be equal in some algorithms. Also, the number of rounds in the algorithm is no less important than the size of the key, as it is an important factor for the encryption and decryption process. Performing more rounds, strengthens the security of the algorithm, but increases the complexity as well. That is why, when designing a cryptographic algorithm, the number of rounds is one important factor that should be set carefully. In the second part, will be discussed some of the newly published papers that used these algorithms to encrypt data in the cloud computing.

### 4.1 ANALYSIS OF ENCRYPTION ALGORITHMS

In this section comparative of encryption algorithms are presented. Encryption algorithms present some factors, these factors are Encryption type, Key length, Block size and number of rounds, key used, Structure of the algorithm. Table 1 shows a comparison between symmetric-key cryptographic algorithms. It displays the name of the algorithm, algorithm developer and year of development, block size, key size, number of round and the structure of the algorithm.

**Table 1.** Comparison of symmetric-key algorithms structure

| Algorithm | Developed By | Block size | Key size | No. Rounds | Structure of the algorithm |
|---|---|---|---|---|---|
| DES | IBM, 1977 | 64 bit | 56 bits | 16 | Balanced Feistel |
| AES | Vincent Rijmen, JoanDaemen, 2001 | 128 bit | (+8 parity bits) | 10, 12 or 14 | Substitution, permutation |
| Blowfish 3DES | Bruce Schneider, 1993 | 64 bit | 128, 192 or 256 | (depending on key size) | Feistel |
| DES | | 64 bit | bits 32–448 bits | 16 | Feistel |

**Table 2.** Comparison of asymmetric-key algorithms structure

| Algorithm | Developed by | Key Size | Structure of Algorithm |
|---|---|---|---|
| RSA | Rivest, Shamir, and Adleman,1977 | 1024, 4096 bits | Integer factorization |
| D-H | Witfield Diffie and Martin Hellman,1976 | 2013,224 bits for q and 2048 bits for p | Key exchange |
| ECC | Neal Koblitz andVictor S. Miller,1985 | 164 bits | Elliptical curve |

## 4.2 COMPARISON OF DIFFERENT PAPERS THAT BASED ON ENCRYPTION ALGORITHMS

Table 3 presents some studies in recent years that deal with the encryption techniques used in the cloud computing security, where it reviews both the study and what are the algorithms used in it, as well as the tools used and the size of the key and what are the advantages of that study.

Table 3. The summary of the reviewed papers in this paper.

| Sr. No | Title paper | Author and Year of published | Algorithm used | Work Proposed | Advantage |
|---|---|---|---|---|---|
| 1 | "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5"[22] | Advit i Chauhan, 2017 | Blow fish-MD5 / hashing | It proposes a new parallel encryption algorithm, mixing and changing MD5 and Blowfish encoding schemes for increased security. | The time of implementation of the proposed hybrid algorithm is lower compared to the RSA-MD5 hybrid algorithm. |

| | | | | | |
|---|---|---|---|---|---|
| 2 | "Secure algorithm for cloud computing and its applications"[23] | Akshita Bhandari, 2016 | RSA-AES | Proposed hybrid encryption uses Rivest-Shamir-dleman (RSA) algorithm and Advanced Encryption Standard algorithm to increase efficiency, consistency and trustworthiness in cloud | Increase the security of encrypted data in cloud servers along Reduce the exhaustion of memory size, cost and time whether in encryption or decryption process |
| 3 | "Enhanced Hybrid Blowfish and ECC Encryption to Secure Cloud Data Access and Storage Policies" [24] | Jobandeep Kaur, 2018 | Blowfish-ECC | Proposed new approachto enhance efficient data access policies for huge data. | Enhance the effective and efficient data access policies for huge data |
| 4 | "A Security Model for The enhancement of Data Privacy in cloud Computing"[25] | Yoshita Sharma, 2019 | AES-RSA | Proposed model provides multi-level encryption which using Hybrid Encryption by combine RSA and AES algorithm | increase the running time of proposed model compare with RSA algorithm |
| 5 | Hybrid Algoriyhm for Clod Data Security [26] | Richa Singla, 2017 | MD5 and AES | Proposed a hybrid algorithm which compriises of MD5 hash with AES algorithm for increased security as well as to reassure users about the security of their data in the | Increased security as well as to reassure users about the security of their data in the cloud. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | cloud | |
| 6 | "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography"[28 | P.Chinnasamy, 2018 | Blowfish, RSA | Proposed hybrid method For storing health-related data in cloud storage, a data is encrypted using Blowfish and keys are managed using the enhanced RSA algorithm.. | Time of proposed hybrid approach for encryption and decryption is better than other methods. Also offered the large prime numbers for key generation and efficient key management. |
| 7 | An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security "[29] | Vikas Goyal, 2018 | AES, SHA-1 and ECC | Designed and implemented hybrid algorithm using the various cryptography techniques such as the AES, SHA-1 and ECC for securing cloud data | Highly secure for all types of sensitive data cloud environment. |
| 8 | A Hybrid Cryptography Algorithm for Cloud Computing Security "[27] | Divya Prathana, 2017 | Blowfish, RSA, and SHA-2 | Proposed hybrid algorithm combines Blowfish, RSA, and SHA-2 algorithms to provide high security. | The combination these algorithm provides high security on data transmission over the internet |

## V. IMAGE PROCESSING CLOUD APPLICATION

In this section, we proposed an image-based cloud computing. The main steps are implemented using Apache version :2.4.55 with server cs20-phk cloud platform by using Apex Crypto Class. This class provides image encryption. The first step uploaded the image as array of pixels values to the Apache Cloud and the encrypt it using the ECC with Hill Cipher encryption algorithm in the cloud storage. We hosted a widget in flutter and then upload the image

to the cloud storage using the API under an account cloud object to encrypt image and the decrypt it. We have implemented ECC with Hill Cipher in term of time comparison Figure 14 shows the main steps of the image encryption based cs20-phx cloud storage.

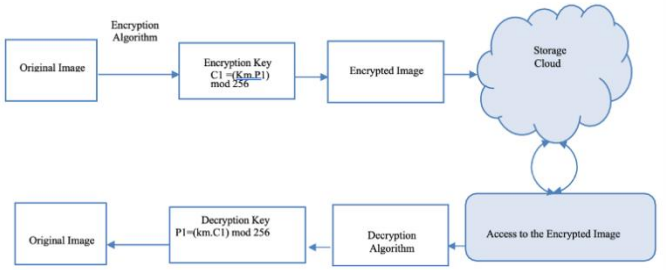


**Figure 15** The proposed image-based cryptography cloud Storage using salesforce.com

Table 4 shows the times in second for different image size with approximately upload rate 2.2Mb/s and download rate 7.3Mb/s, image type .bmp.

## VI. CONCLUSIONS

This paper represents a comprehensive study of the main types of encryption technologies and their algorithms, symmetric-key algorithms, asymmetric-key algorithms, hashing algorithms and hybrid algorithms. In symmetric-key algorithms the algorithms DES, 3DES, Blowfish and AES are explained. In symmetric-key algorithms the algorithms RSA, H-D and ECC are explained. In hashing algorithms MD5 and SHA are explained. Each algorithm aims to introduce extra level of security and to satisfy performance requirements more than earlier proposed algorithms solution. This extra security level should balance between a robust algorithm structure and a reasonable complexity computation and to choose the suitable cipher algorithm to protect data in the cloud environment as its multitenancy platform and jeopardize by many attackers. The application of cloud image-based cryptosystem is implemented and time results are shown which show a good performance using salesforce.com cloud storage.

## VII. REFERENCES

[1]. Tyagi M., Manoria M., Mishra B., "A Framework for Data Storage Security with Efficient Computing in Cloud", In: Kamal R., Henshaw M., Nair P. (eds) International Conference on Advanced Computing Networking and Informatics. Advances in Intelligent Systems and Computing, vol 870. Springer, Singapore. 2019.

[2]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Information Technology Laboratory, 2011.

[3]. Jassem, Yasser Hassen, And Alharith Abdulkareem Abdullah. "Enhancement Of Quantum Key Distribution Protocol For Data Security In Cloud Environment.", Icic International, Volume 11, Number 3, March 2020.

[4]. Shankarwar M.U., Pawar A.V., "Security and Privacy in Cloud Computing: A Survey", In: Satapathy S., Biswal B., Udgata S., Mandal J. (eds) Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Advances in Intelligent Systems and Computing, vol 328. Springer, Cham, 2015.

[5]. Mehdi Ebady MannaMoahmmed Ali Mohammed A, " Data Encryption Scheme for Large Data Scale in Cloud Computing", Journal of Telecommunication 9(2-12):1-6, September 2017.

[6]. Y. Al-Dhuraibi, F. Paraiso, N. Djarallah, and P. Merle, "Elasticity in Cloud Computing: State of the Art and Research Challenges," IEEE Trans. Serv. Comput., vol. 11, no. 2, pp. 430–447, 2018.

[7]. Mehdi E. Manaa and Rasha H. Jwdha "a proactive data security scheme of files using minhash technique", Journal of Theoretical and Applied Information Technology 96(24):8421-8433, December 2018.

[8]. S.Sandhya, U.Reshma and Dr.V.Praveena, " Survey on Various Data Encryption Algorithms Used in Cloud Security"

[9]. W. Stalling, "Cryptography and network security principles and practices", Fourth Edition, Prentice Hall, December 2006.

[10]. Elgeldawi, Enas, Maha Mahrous, and Awny Sayed. "A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey", International Journal of Computer Applications 975: 8887, 2019.

[11]. Privacy." Scientific American", vol. 228, no. 5, pp. 15-2, 1973.

[12]. FIPS PUB 46-3, “Data encryption standard (DES),” National Bureau of Standards, U.S. Department of Commerce, January 1977.

[13]. Nigoti, Rashmi, Manoj Jhuria, and Shailendra Singh. "A survey of cryptographic algorithms for cloud computing." (2013).

[14]. Tamilselvi.S, " Data Storage Security in Cloud Computing Using AES" , International Journal of Advanced Networking & Applications (IJANA) Volume: 08, Issue: 05 Pages: 124-127, 2017.

[15]. Advanced Encryption Standard", En.wikipedia.org, 2020. [Online].Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 28- 5- 2020].

[16]. C.Gentry and S.Halevi. “Public Challenges for Fully Homomorphic Encryption” TBA, 2010.

[17]. Gupta, Utkarsh, Mrs Shivani Saluja, and Mrs Twinkle Tiwari. "Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms." 2018.

[18]. ChaitaliHaldankar, Sonia Kuwelkar,“IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM” IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014.

[19]. Jirwan, Nitin, Ajay Singh, and Dr Sandip Vijay. "Review and analysis of cryptography techniques." International Journal of Scientific & Engineering Research 4.3: 1-6, 2013.

[20]. Thivagar, L. M., Hamad, A. A.," Conforming Dynamics in the Metric Spaces." J. Inf. Sci. Eng., 36(2), 279-291, 2020.

[21]. Thivagar, M. L., & Abdullah Hamad, A." a theoretical implementation for a Proposed Hyper-Complex Chaotic System." Journal of Intelligent & Fuzzy Systems, Vol.38,no.3, pp.2585-2590,2019.

[22]. Chauhan, Adviti, and Jyoti Gupta. "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5." 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2017.

[23]. Bhandari, Akshita, Ashutosh Gupta, and Debasis Das. "Secure algorithm for cloud computing and its applications." 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence). IEEE, 2016.

[24]. Jobandeep Kaur, Dr Vishal Bharti2 and Mr. Shamandeep Singh, “Enhanced Hybrid Blowfish and ECC Encryption to Secure Cloud Data Access and Storage Policies”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 5, May 2018.

[25]. Sharma, Yoshita, Himanshu Gupta, and Sunil Kumar Khatri. "A Security Model for the Enhancement of Data Privacy in Cloud Computing." 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE, 2019.

[26]. Singla, Richa, and Richa Dutta. "Hybrid Algorithm for Cloud Data Security.", Volume-10, Number-2 Jan-June 2017.

[27]. Timothy, Divya Prathana, and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS). IEEE, 2017.

[28]. Chinnasamy, P., and P. Deepalakshmi. "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography." 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2018.

[29]. Goyal, Vikas, and Chander Kant. "An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security." Big Data Analytics. Springer, Singapore, 195-210, 2018.

**Cite this article as :**

Mamta Khanchandani, Dr. Sanjay Buch, "Effectual Cryptography Approaches for Cloud Storage Image Encryption", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 2, pp. 281-294, March-April 2023. Available at doi : https://doi.org/10.32628/IJSRST52310245
Journal URL : https://ijsrst.com/IJSRST52310245