iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** VIII **Month of publication:** August 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.37783

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com*

# A Survey on Performance Evolution Of Various Encryption Algorithms

Pranjal Soni[1], Amit Kumar Sariya[2]
[1]*Dept. of Computer Science and Engineering, Alpine Institute of Technology, Ujjain, M.P.- 456010, India*
[2]*H.O.D, Dept. of Computer Science and Engineering, Alpine Institute of Technology, Ujjain, M.P. - 456010, India*

***Abstract:*** ***Security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. In this paper we are studying the performance evaluation of the various encryption algorithms and also we are analyzing the best encryption algorithm from the widely used algorithms.***
***Keywords: Cryptography, Encryption Algorithms, CPU Time, Computation Time***

## I. INTRODUCTION

Due to many crucial services such as banking and eWallets(Paytm, PhonePe etc), being available as web and mobile applications, security is a major aspect which has always been a key area of consideration for banks and companies to protect unauthenticated users from illegal activities and transactions. In the current world, there are numerous encryption algorithms available in the market to be used for security. The time taken by an encryption or decryption technique to encrypt or decrypt data of some size with a key of some size can be taken as a prominent parameter to decide the excellence of an algorithm in addition to its security. The quest for the best solution to offer necessary security from hacker attacks to the data that is exchanged over the internet or the other media types is currently in trend. As far as the security of data is concerned cryptography comes in rescue that deals with secret (crypto-) writing (-graphy) that is to conceal the data from the reach of all except the sender and the intended receiver. Cryptography encompasses numerous techniques that can be used to encrypt or decrypt some data. We have symmetric-key as well as asymmetric-key algorithms. Even choosing a symmetric-key algorithm to secure the data opens a wide range of algorithms to choose from. Our major concern is to choose the most efficient one with good performance accompanied by good security. Studying the performance and behavior of such algorithms with varied sizes of data and keys helps us in choosing the right algorithm as per our needs.

## II. CRYPTOGRAPHY

Cryptography is the method of keeping information secure by transforming it into form that unintended recipients cannot understand. In cryptography, an original human readable message, referred to as *plaintext*, is changed by means of an algorithm, or series of mathematical operations, into something that to an uninformed observer would look like gibberish; this gibberish is called *cipher text*. These Algorithms which are used to covert a plain text into cipher text is referred to as Encryption Algorithms.

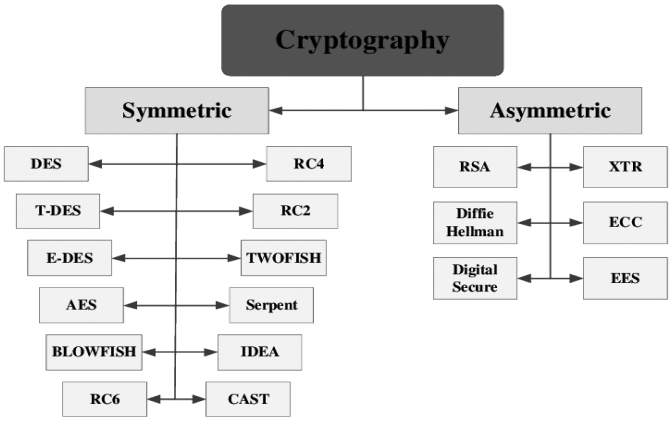


Figure 1. Cryptography types based on Symmetric key and Asymmetric key

## III. ENCRYPTION

In cryptography, encryption is the process of encoding a message or information in a way that only authorized parties can access it and those who are not authorized cannot. Encryption is the method by which information is converted into secret code that hides the information's true meaning.

## IV. ENCRYPTION TYPES

There are mainly two types of Encryption as follows :

### *A. Asymmetric Encryption*

In public-key encryption schemes, the encryption key is published for anyone to use and for encrypting messages. Only the receiving party has access to the decryption key that enables messages to be read. Public-key encryption was first described in a secret document in 1973. Before that, all encryption schemes were symmetric-key (also called private-key).

### *B. Symmetric Encryption*

In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication.

## V. ENCRYPTION ALGORITHMS

There are different Encryption Algorithms available which are as follow[1]:

### *A. DES*

Data Encryption Standard was developed in March 1975 by IBM. This is one of the earliest algorithms to be used at such a commercially large scale to protect data. Over the years, due to its small key size and the need to transfer data, it was phased out [1]. Data Encryption standard is based on the Feistel structure concept. A 64-bit block goes through 16 rounds and
uses a key of length 56-bits to produce a ciphertext .The Key originally has a size of 64-bits (equal to the block size) but in every byte, 1 bit is used as a parity bit and hence isn't used for execution. The 56-bit key is the permuted into 16 subkeys of 48-bits each, used for the 16 rounds. 8 Sboxes are used in the process and the same algorithm in reverse is used for decryption [1].

### *B. TDES*

Triple Data Encryption standard developed in1986, was created to remove some of the limitations of theoriginal DES algorithm without making any modifications tothe internal components of the DES encryption system [1]. TDES as the name suggests, uses the DES algorithm thrice on the data block to produce an equivalent ciphertext. As no changes are made to the internal structure of the DES algorithm, TDES still follows the Feistel Structure concept. TDES uses two or three keys in an encrypt-decryptencrypt sequence to provide a valid ciphertext. The reverse of the operation is done to convert the ciphertext to plaintext. TDES uses a 64-bit plain text, 48 rounds and a key length of 168-bits with the use of 8 S-boxes to provide an equivalent 64-bit ciphertext [1].

### *C. Extended DES*

The extended DES was designed by Rajay R Pai, Seung J. Han and Menahem Lowy and this algorithm was created to remove the security issues in thetraditional DES algorithm while changing the architecture of the algorithm [1]. The encryption algorithm for the EDES. Each block of data consists of 96-bits that are divided into three equal sub-blocks (A, B and C) each containing 32-bits. A different f-function is performed for each of the following three sub-blocks and the number of S boxes generated is increased from 8 to 16. A bigger key of each 56-bits long: K1 on the left and K2 on the right. After the first permuted choice (PC-1) each of the 56-bit keys is further divided into left and right keys both of 28 bits each and so on the process is continued for the next 15 rounds.

### *D. AES (Rijndael)*

Also known as Rijndael, was developed By Joan Daemen and Vincent Rijmen for the U.S.as its new Encryption standard in October of 2000. It provesan effective resistance against crypto-analytic attacks. AES isthe actual name of the standard that was used by the United States and Rijndael is the specific algorithm, but it is most widely known as AES [1]. AES is another symmetric key encryption algorithm that uses a 128, 192, 256-bit, plain text that is put through a variable 10,12 or 14 rounds respectively (Default number of rounds=key- length/32+6).this block cipher. Each round has 4 basic functions to be performed namely: 1. Sub bytes, 2. Shift Rows, 3. Mix Columns, 4. XOR nth round key. The last round is the same except for the fact that the Mix Column process is eliminated.

*E. Twofish*

The Twofish encryption algorithm was created by Bruce Schneier, and was one of the five finalistsnominated to be the United States new encryption standard atthe Advanced Encryption Standard contest, but did not getselected for standardization. Twofish is related to the earlierblock cipher Blowfish. As of December 2017, Twofish hasnot been patented and is an open source code [1]. Based on the Feistel Structure, Twofish is also another symmetric key algorithm. This block cipher uses 128-bit plain text and processes it through 16 rounds using a key of variable lengths such as 128,192,256 bit. It also uses 4 S-boxes during the process. The algorithm is reversed to convert the ciphertext back into its corresponding plaintext.

*F. Blowfish*

Blowfish is a symmetric block cipher that can replace IDEA or DES as a drop-in replacement. Designed by Bruce Schneier in 1993 Blowfish is a free alternative to many of the present algorithms[1].

*G. Modified Blowfish*

This algorithm was developed to remove some issues related to security and processing the speed by changing the f-function calculation but keeps the structure of the algorithm the same [1].

## VI. LITERATURE SURVEY

Literature review presented here is for the comparison of various encryption algorithm to find out an efficient algorithm . Encryption Algorithm is the method of converting a message into unreadable form to secure the message from unauthorized access. There are different Encryption algorithms available for encrypting the message. Here is the survey of various researches on different Encryption Algorithms.

*A. "A Comprehensive Analysis Between Popular Symmetric Encryption Algorithms"[1]*

There are many different types of symmetric encryption algorithms such as DES, TDES, Blowfish, AES (aka Rijndael), Twofish. Asymmetric encryption uses two different keys namely the private key and the public key to help in achieving encryption or decryption. The sheer hostility of the network in question shows us the need to secure information before it to be transmitted over the network. The advantage key encryption is that the confidentiality of the data in question relies on the key and not the algorithm using the key. This means that even if the attacker knows the decryption algorithm, decryption isn't possible unless the attacker knows the key as well. Encryption algorithms can be primarily divided into two types, symmetric and asymmetric key algorithms. Figure 5 shows the Encryption system Hierarchy. Symmetric encryption process uses only a single Private Key to encrypt as well as decrypt data. The different asymmetric encryption algorithms are PGP, RSA, SSH and many more. This paper primarily targets its research towards popular symmetric key Encryption algorithms based on specific criteria. Nowadays it is very important to protect the data transmitted over the internet due to the increasing number of cases in which data to confidential between two parties is stolen by intruders.

As per [1] The parameters that affect the selection of a certain cipher for a particular application are:

1) *Architecture:* Defines the basic structure that encompasses how a certain algorithm their respective plain text into its corresponding ciphertext. Based on the usage of a specific key (either secret or public key) we also are able to determine if the algorithm is symmetric or asymmetric.
2) *Security:* Defines how strong the encryption algorithm is against an attack. Encryption systems strive to satisfy this particular criterion and hence security has become an important criterion among these parameters. Secure encryption generally use bigger key sizes than its less secure counterparts.
3) *Efficiency:* A major criterion on which encryption algorithms are analysed. Efficiency basically depends on two factors such as speed of execution and memory utilization.
4) *Limitations:* Defines the already known attacks that the encryption is vulnerable to. Helps to decide whether the encryption algorithm must be used or not for a specific application.

*B. "Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems" [2]*

By increasing the speed of data processing process by computer systems, the Blowfish Algorithm is capable of creating and developing a larger and larger length that ensures system security. In Cryptography, Twofish algorithm it's symmetrical block algorithm whose block size it's 128 bits, and the key size changes to 256 bits. This algorithm associated with the predecessor Blowfish algorithm. Blowfish is a variable-length key algorithm with 64-bit block cipher; was created in 1993 by Bruce Schneider to replace the DES (Data Encryption Standard).

*C. "S-DES: An efficient & secure DES variant," [3]*

The design criteria for DES were not published and some modifications were introduced, which reduced the security level of DES such as reducing the size of the secret key from 128 to 56 bits. This modification was the reason behind breaking DES after 20 years. DES uses the classic uniform Feistel Network and has a block size of 64 bits and a key size of 56 bits. The secret key consists of eight bytes, however, one bit of each byte is dropped, which means that the key size is effectively 56 bits. The input block (64 bits) is separated into 2 sub-blocks (words): the 32 leftmost bits part L and the 32 rightmost parts R . Then, the round function is applied 16 times and for each round a new L and R are produced. The proposed S-DES variant should be strong enough to guard against the most known types of attacks such as statistical, differential, chosen/known plain-text, and brute-force attacks. In fact, doubling the size of the data block and the secret key doubles its resistance against analytical and brute force attacks. The original DES cipher scheme suffers from several security weaknesses, while 3DES suffers from performance issues. This motivated the work to define a new efficient and secure DES variant, S-DES. Indeed, the newly proposed variant employs an extended FN with a 125-bit block size. In addition, the size of the secret key of S-DES is 112-bite. Therefore, S-DES provides better resistance against attacks such as brute-force, differential, and linear cryptanalysis.

*D. "Enhancing data security using DES-based cryptography and DCT-based steganography,"[4]*

One of the main problems in digital communication is the security of the data was transmitted over the internet network. Data can be stolen or accessed by attackers with certain techniques. Therefore, it is the necessary application of reliable data security techniques for data exchange via internet media.

Cryptography and Steganography are two of the most commonly used to secure digital data. Cryptography is a technique for securing data where the original data is randomized in such a way that it is difficult to understand. Original data can only be opened by a specific person using predefined custom keys. The applications generated in this research[4] are able to secure data or document files such as word files (.doc, .docx), excel files (.xls, .xlsx), powerpoint (.ppt, .pptx) files, and pdf files. Meanwhile, the combination of the DES cryptographic and DCT steganographic methods proved to improve data security because it has two levels of security.

Based on the experiment can also be concluded that the stego-image quality can still be in a good category with an average value of PSNR of 46.9 dB. The combination the two methods resulted in a computation time of 0.75 milliseconds/bytes. The computational time still needs to be improved in the future research. Overall, the success rate of the proposed method in securing the data was 58%.

The success of the data security process depends on the resolution of the cover image used. In this study, it is recommended to use a cover image resolution of 1024 x 720 or more. One research[4] provides a data security application that can be useful for improving the security of data files before being sent over the public network. In the next study, the computation time needs to be optimized again so that it becomes faster. Also, an increase in file size of 4.79 times can be reduced by adding a compression method or optimizing the encryption algorithm used.

*E. "Fast software implementation of des for lightweight platforms"[5]*

Many lightweight cryptography protocols have not designed to be efficient on software platforms, since designers are usually focused on hardware requirements. This study addresses this problem. We present a new design architecture for improving the software implementation of the DES. The DES is a family of block ciphers. It is efficient in hardware but its design was not oriented for software platforms. Aim of our proposed design is to find a block cipher architecture design for lightweight applications. Data Encryption Standard (DES) is a symmetric key encryption algorithm. The importance of DES is the most commonly used block encryption algorithm in the world for 30 years. It was accepted as a standard in 1976, and this standard published as FIPS 46 in 1977[5].

*F. "An efficient implementation of enhanced key generation technique in data encryption standard (DES) algorithm using VHDL"[6]*

The need of cryptography is emerges to keep the private data from unapproved individual. Security of the information or framework is relies on upon both cryptographic calculation and key utilized for encryption/decryption. Cryptography is required in different areas like banks, military, railroads, media transmission and so forth. In electronic reserve exchange like ATM cards, computer passwords, electronic passwords likewise require the security.

The route toward changing over plain substance to figure content is known as encryption and the count which encodes the data is known as encryption computation. In the present day cryptography, a mix of both open key and regular symmetric cryptography is used. The reason behind this is open key encryption arranges are computationally genuine versus their symmetric key accomplices. Due to the dynamic key generation unit secrecy of the key get increased. Simulation results are shown for both encryption and decryption.

Using proposed design, we can achieve high speed and reduced logic complexity which gives enhanced DES algorithm. According to this enhanced DES algorithm has broad application area in secure data communication and transmission. In future, we can execute this framework for greater security in various applications, for example, Smart card security Database administration framework, Set top box, Wireless correspondence security, Content insurance. The security of any type of algorithm is dependent on the secrecy of the key[6].

*G. "Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations"[7]*

One of the significant issues is file management. Secure file management has become an important technology along with the increasing use of computer systems. The recommended file security is storing encrypted files to be inaccessible to irresponsible people. With the rapid development of network technology, attacks over the Internet are also diverse, traditional encryption algorithms (single data encryption) is not enough to ensure information security on the internet. According to [7], AES (Advanced encryption standard) is the best encryption algorithm, that was proposed by NIST. On the other hand, Blowfish is the fastest algorithms, but the security level is lower than that of AES. Message Digest 5 (MD5) hash function is proposed by Rivest to improve the previous version MD4 and published in 1992. MD5, similar to other cryptographic hash algorithms, retrieves messages of a free size and produces fixed-size output ( 128 bit). Blowfish was designed by Bruce Schneider in 1993 as an alternative algorithm for rapid encryption. Blowfish is included in 64-bit Chipper block encryption with a key length of at least 32-bit to 448-bit. Made for use on computers with large microprocessors (32-bit and above with large data cache). In this study, the authors tried to compare the combination of Blowfish and AES 256 algorithms with AES 256 and Blowfish for the fastest time of encryption and decryption. Differences in the order of combinations of algorithms will be observed at their safety level.

*H. "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing"[8]*

The adventure and consumers have transferred the information using cloud facility to minimize the data execution cost and cost of the storage facility. However, the information is lost due to sensitivity, to reduce the information drop the information are encrypted before loading the information into the cloud. The conversion of plain text to ciphertext is called encryption, and the reverse process is called decryption. Privacy as a Service is used to protect storage and handling of users' private data[8]. The AES based cipher text retrieval provides more security.

But the proposed system using elliptic curve key for key generation and encrypt the data using blowfish. So the blowfish algorithm provides high throughput than others. During the implementation, we notice that proposed approach achieved the efficiency at the Data Owner side and user side.

This work allows a user to search keyword over the encrypted data. So the blowfish encryption is important in storage and retrieval of outsourced cipher text

Then the Blowfish decryption algorithm is used to get the plain text. It provides security for outsourced data, and the performance of the proposed work showed better efficiency regarding of low computation and communication costs. To search the ciphertext content effectively, Porter stemming based index has generated and the data stored on a cloud as encrypted form. Here Blowfish encryption and elliptic curve keys are used for secure data transmission. When the authorized user generates a query to the cloud, the relevant files are sent to the user in an encrypted format. Then the user gives the private key for decryption process, and blowfish decrypt the files. This proposed method provides better performance by comparing with the conventional algorithms in the way of retrieval efficiency and less time-consuming[8].

*I. "Comprehensive study of symmetric key and asymmetric key encryption algorithms"[9]*

Cryptography attracted many researchers. Reversion this cipher data to original data called decryption process. Cryptography is widely used to secure data in cloud computing. Due to the extensive use and sharing of data in the Internet, it is necessary to protect data from hacking, noise, and interference.It is used for protecting information during transmissions between users. It alters the content of transmitted data to unreadable form, once received by the receiver, it is converted back to its original form. Encrypting data results to an unreadable format called cipher-data. Cryptography had a set of security goals to ensure the privacy of data. These goals are confidentiality, authentication, data Integrity, non-repudiation and access control[9].

It is classified into Symmetric (private-key) and Asymmetric (public key) keys encryption. Examples of Symmetric algorithms are DES, 3DES, AES, Blowfish and DSA (Digital Signature Algorithm), Elliptic Curve, Diffie- Hellman (key exchange) and RSA are examples of Asymmetric algorithms. Encryption is a technique for protecting sensitive data. It hides the sensitive data of users by using the same key to cipher and decipher the data.

The following four algorithms uses symmetric encryption -

*1)* Data Encryption Standard (DES)
*2)* Triple Data Encryption Standard (3DES)
*3)* Advanced Encryption Standard (AES)
*4)* Blowfish

One research proposed performance evaluation for four encryption algorithms (DES, 3DES, Blowfish and AES). They used different settings to evaluate encryption algorithms such as different sizes of data blocks and decryption speed under different hardware and software platform. All codes implemented in C++, .NET(2003) and run on a Pentium- 4, 2.1 GHz processor under Windows XP SP1. They showed that Blowfish was the best algorithm in case processing time and it had strong key size(448 bit). AES needed more processing time when data block size was relatively large. 3DES required more time than DES. Also, they showed that AES was the best algorithm in cases number of requests executed per second in different user loads, and in the response time in different user load situation performance results of stream cipher. Another research made a comparison of the performance of algorithms (DES, AES, and Blowfish). They concluded that Blowfish gives the best results in various block cipher modes with minimum weak points. AES showed poor performance compared with other algorithms. In general, symmetric encryption algorithms are faster than asymmetric encryption algorithm but it had only one weak point that it is shared its key with other parties involved in the process. Asymmetric encryption has a strength point that it is used two different keys but it's required more processing time than symmetric encryption. In the survey[9], they give a detailed study of symmetric like AES, DES, 3DES and Blowfish also for asymmetric algorithms such as RSA, DSA, Diffie-Hellman and Elliptic Curve. According to an analysis section, we found that the efficiency of the various algorithms is affected by the difference parameter. In the current state of increasing demand on cloud application, it became necessary to provide efficiency, robust and high-security algorithms that suitable with the large scale of data in the cloud. Speed and security are the most important rules play on cloud applications[9].

*J. "An Enhanced BlowFish (eBf) Algorithm for Securing x64FileMessage Content"[10]*

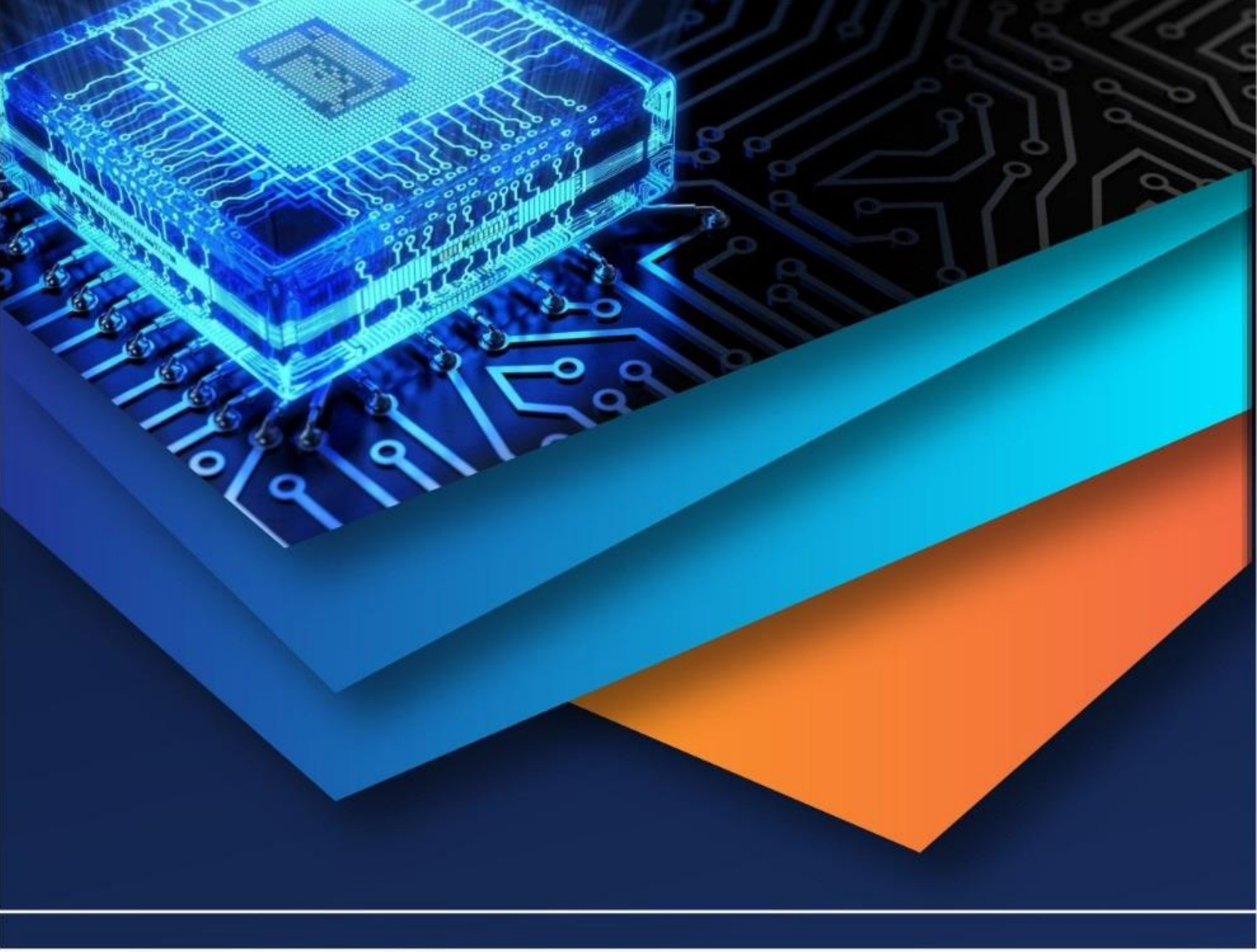
Currently, there are various techniques and methods designed for specific problem. Encryption of data over the network is one of the key methods which translates information that only authorized user has the knowledge of the secret key. Everyday new techniques are developed with high security rate of protecting and securing confidential information. Over the years, the scope of cryptography has widen and evolved with the modern transactional requirements. The need to protect data has become more complex as computers were introduced and cryptanalysis has adapted to the increasing complexity of cryptography or the technique of enciphering and deciphering messages that maintains the privacy or security of data. There is a general need for enciphering all data sent between computers connected to a network. Computer systems must have a means to prevent unauthorized access to avoid any alteration or worse loss of data between devices connected to the network. Basically, blowfish encryption algorithm contains 16 rounds. Each round consists of XOR operation and a function (F).

## VII.CONCLUSION

During the literature survey, we have identified various pros and cons of different encryption algorithms but it attracts a comparative study of DES, Blowfish and Twofish algorithms together to assess which one will perform better in real life scenario when compared for encryption and decryption on the same files. We have also covered various other encryption algorithms above which reside as competitors for these algorithms but we want to study these three algorithms to be specific. If we choose the speed as a prominent factor to decide the efficiency of these techniques to encrypt/decrypt data of different sizes using the same key or data of fixed size using different keys with different sizes, we shall be able to draw significant conclusions.

## REFERENCES

[1] S. S. Ghosh, H. Parmar, P. Shah and K. Samdani, "A Comprehensive Analysis Between Popular Symmetric Encryption Algorithms," 2018 IEEE Punecon, Pune, India, 2018, pp. 1-7.
[2] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, A. Fesenko and A. Abisheva, "Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems," 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 970-974.
[3] M. Noura, H. N. Noura, A. Chehab, M. M. Mansour and R. Couturier, "S-DES: An efficient & secure DES variant," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, 2018, pp. 1-6.
[4] Solichin and E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," 2017 3rd International Conference on Science in Information Technology (ICSITech), Bandung, 2017, pp. 618-621.
[5] F. Özkaynak and M. I. Muhamad, "Fast software implementation of des for lightweight platforms," 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, 2017, pp. 1-4.
[6] P. M. Chabukswar, M. Kumar and P. Balaramudu, "An efficient implementation of enhanced key generation technique in data encryption standard (DES) algorithm using VHDL," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 917-921.
[7] M. A. Muin, M. A. Muin, A. Setyanto, Sudarmawan and K. I. Santoso, "Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations," 2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2018, pp. 137-141.
[8] S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 267-271.
[9] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), Antalya, 2017, pp. 1-7.
[10] G. L. Dulla, B. D. Gerardo and R. P. Medina, "An Enhanced BlowFish (eBf) Algorithm for Securing x64FileMessage Content," 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), Baguio City, Philippines, 2018, pp. 1-6.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY