iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43500

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: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Secure Cloud Storage Using Different Algorithms in Cryptography

Dr. Sudheer. S. Marar[1], Jolsana Maria Joyson[2], Mr. Ashish L[3]
[1]*Professor, and HOD, Department of MCA, Nehru College of Engineering and Research Centre*
[2]*Department of MCA, Nehru College of engineering and research Centre*
[3]*Assistant professor, Department of MCA, Nehru College of Engineering and Research Centre*

Abstract: ***Cloud computing offers online services that allow visible servers, dynamic reminiscence swimming pools, and so for a smooth get right of entry. Because dispensed computing is based on the internet, security concerns include information protection, confidentiality, records protection, encryption, and authentication seem. Cloud records garage protection is a primary difficulty. In this examination, we aimed to explore a variety of information safety strategies. The use of cryptographic algorithms is used to solve information protection and privacy troubles in cloud storage. Inside the proposed Hybrid set of rules system RC4, DES & AES Algorithms have been used to enhance data security and privacy. Proposed hybrid system algorithm shield upload and download of statistics from cloud garage. In this case, mystery keys are required for each encryption to do away with encryption. As a result, several parameters have calculated the usage of taking a look at features that encompass encryption time, memory utilization, privacy length, and output to illustrate the performance of the hybrid machine, facts simulations are to be supplied to JAVA, the use of the Eclipse IDE device. The proposed hybrid machine set of rules is used and tested the usage of various record formats such as textual content and photo data. The proposed set of rules is thought to paintings properly to provide additional information safety.***
Keywords: Cryptography, cloud computing, encryption/decryption Algorithm

I. INTRODUCTION

Cloud computing provides cloud services online. The Cloud computing model allows apps once information is accessed remotely. Three levels of services used are d to define as cloud computing infrastructure as a service (IaaS), Software as a service (SaaS), and Platform as a Service(PaaS). IaaS provides visual equipment and storage to users. SaaS provides users with frameworks to improve cloud hosting applications to develop, use, analyze, and manage theorem services. PaaS provides users with services and applications with a web browser anywhere at any time and any place. Data security is a major issue as data is being held is a third party, and the risk is high if users gather information in transparent manner storage also provides a backup tool. Cloud is divided into three categories. There are a public cloud, virtual cloud, and hybrid cloud cloth most popular security issues in cloud computing are data recovery issues, data privacy, Integrity, Availability, Confidentiality, Operational privacy, unauthorized access to such management interface, vulnerability in virtual machine(VM)script illustration, data leakage risk, challenges with security metrics &monitoring, Trouble regarding digital key management & numeric codes Cloud interoperability problem, and monitoring activity patterns. Cryptography refers to the process of converting plain text into unreadable text Cryptography might be used to identify users as well as safeguard data from theft and modification. Cryptography contains three categories: secret key (symmetric) cryptographic public-key key (asymmetric) cryptography, as well as hash functions. Public key encryption is referred to as symmetric key exchange in the middle of the transmitter as well as the receiver of data. In Asymmetric key cryptography, public-key encryption is a kind of encryption that employs two distinct keys, one for encryption (public key) and decryption (private key). The public key, everyone knows, and the private key, then only the owner knows For cryptography, the following three algorithms were proved to be effective in terms of encryption/decryption time and other parameters for cloud storage: DES is an algorithm program that takes a fixed-length stream of plaintext bits as well as, apparently limiting decoding to those who aware of the encryption key takes a secure block size of 128,192, or 256 bits. The cipher is defined as many transformations Long repetitions that transform the input of the cipher text's last output. Each round involves multiple processing steps, together with one that relies on the encryption key. A series of reverse rounds are applied to turn the ciphertext again into plain text just using the same encryption key. Rivest Cipher four (RC4) is a symmetric-key block cipher invented by Ron Rivets. The RC4 algorithm performs bit-wise encryption and decryption with a key length of 40-128 bits.

The RC4 algorithm is widely used to secure the transport layer. Because The Rivest cipher four is still a stream cipher, it produces streams of bits, with each byte of the same text to be encrypted. The password for data encryption is called the secret key. These algorithms are less efficient in providing full-time security to cloud data. As these algorithms work individualities are supposed to be less effective in furnishing full-time security to pall data. To ameliorate the effectiveness mongrel system of the named algorithms was conducted for high-position security. This exploration substantially focuses on the performance evaluation of different algorithms for the security of pall storehouse and provides a comparison of cold-blooded security encryption systems with every single algorithm.

II. LITERATURE REVIEW

Described Information technology was used in a variety of ways in nearly every element of life. As it stands, applicable security has always been a major concern that requires further attention. To guard and cover shared and sensitive data, various strategies have been used. This study concentrated on cryptography as a means of achieving zero forbearance for data in vehicle security. Still, the Private or Secret Pivotal Encryption Structure must be named as the mode for administering security to meliorate the security and effectiveness of the system of vital data.

This study concentrated on cryptography as a means of achieving zero forbearance for data in-vehicle security Likewise, to increase the security and effectiveness of essential data, the Private or Secret Pivotal Encryption Structure must be chosen as the paradigm for administering security. This study trouble established three encryption ways analogous to DES, AES, and EB64 algorithms and compared their performances on both encryption and decryption processes predicated on the assessment of encryption and decryption time supplied at each separate experimental step. The trial findings were used to assess the effectiveness of each algorithm on a cell phone.

The results of the numerous studies for SMS plaintext encryption and decryption reveal that EB64 encryption and decryption time is faster than AES and DES. There are various advantages to cloud computing, as well as a few security issues. This study addresses the numerous data security risks that arise when using cloud computing in a multi-tenant environment, as well as potential solutions. This study also goes over cloud computing principles including deployment and service delivery methods. Data leakage or corruption can destroy people's trust and lead to the business' collapse in any commercial or Cloud Computing setting. Many businesses use cloud computing, either directly or indirectly, therefore any data breach in cloud computing affects both cloud computing and the company's operations.

This is one of the main reasons why cloud computing companies are paying more attention to data security. Sharma et.al.,[7]discussed that Cloud computing is becoming increasingly popular in today's environment. used in a variety of settings, including industry, military colleges, and others, must be able to store a large amount of data On the user's request, we can retrieve data from the cloud.

To save data on the cloud, we had to solve many problems. There are numerous approaches to providing a solution to these problems. Many challenges arise when storing data to address these concerns, we use a hybrid cryptography methodology. A fundamental method is ineffective for high-level data security in cloud computing. To achieve block-wise security, this system employs the AES, DES, and RC2 algorithms.

The stenography approach is used to secure key information for all algorithms with a key size of 128 bits. The key information specifies which algorithm and key are used to encrypt particular parts of the file. Distributed computing is a novel and fast-growing set of IT services delivered to a client over the internet on a rental basis, with the option to scale up or down management requirements. It makes use of the power of web-based processing and how information, data, and other assets may be exchanged with clients via PC or mobile devices. This audit has been focused on how to securely store data and information in distributed storage, as well as what measures have been made to address security concerns.

III.MATERIALS AND METHODS

Cryptography on most levels is better than using one algorithm. We need to use a combination of algorithms for that they are compatible with each other. In hybridization, we use AES, DES, and RC4 algorithms. Encrypting data using a hybrid system algorithm is the first step and after sending it to Encrypt file via key encryption and access cryptographic content form using cloud service.

We need to make sure that keys are then encrypted to encrypt data. After The key to encrypt the encryption process is applied to the cipher data through the concealment process. It consists of two types of components described in table 1.

UPLOAD COMPONENTS	DOWNLOAD COMPONENTS
Authentication: Authentication: Users authenticate themselves with their special username and password to the cloud	
Upload: This control system allows people just to have one's documents securely uploaded. Such an entry point uploads the encryption key of that information towards its database of cloud documents.	Download: The user one's documents securely receive the decrypted data uploaded. Such an entry from the Cloud, which point uploads the encryption includes the original text. key of that information (file)
Key Generation: The creation of keys is based on the system's scheduling.	
Encryption: With the uploading, the data is initially put in storage in a temporary server file located in the cloud. Use the user's public key for encryption technology as well as encryption to store the data.	Decryption: When the client wants his protected information to also be downloaded. He/she is asked to enter his password along with the hidden unique number. Then the cloud decodes the data then using the secret key of both the user.

Table1

A. Data Collection and System Requirements

Plain text/File/image data selected under a public cloud model. The text file is selected as a dataset to get the desired results of the hybrid system of algorithms for the security purpose of cloud storage. Image is selected as a dataset to get the desired results of a hybrid system of algorithms for the security purpose of cloud storage the suggested system analysis was carried out in the JAVA programming language. Table 2 describes the software and hardware system requirements for the implementation of the designed system.

Table2.Software and Hardware Requirements

Software Requirements	Hardware Requirements
Java language	RAM: 2 GB or above
Eclipse IDE (V-2020)	CPU: 32 bit OS or above

B. Perpetration Procedure

The following is the procedure for the proposed system

1) Admit that data is trained for encryption & transfer towards others.
2) Also the stoner browses as of native storehouse to choose a train/ image to always be uploaded.
3) After that, the stoner chooses the encryption algorithm they want to use.
4) The proposed system gives druggies the option of employing an admixture of AES, DES, as well as RC4.
5) The named train is uploaded after it has been translated with the encryption algorithm that contains a combination of three algorithms.
6) Accepting the stoner's DES key
7) Gain this same AES key procedure
8) Data file encryption has been done using the AES Fashion
9) Encryption using the DES system with an AES key.
10) Ciphertext/ image using RC4
11) Lines Transferring Process
12) Lines accepting the process
13) Approved translated AES secret key for decryption process we used the DES system
14) Accepted RC4 translated data train decryption using AES system
15) Now the translated train generated
16) So download the translated train

C. Experimentation of Mongrel System

This suggested mongrel cryptography fashion is designed to cover information and data transferred over the internet. The mongrel cryptography algorithm is to cipher as well as secure data effectively. In the suggested mongrel cryptography fashion, three encryption ways were applied. These styles are cold-blooded, and they're used to increase the encryption algorithm's effectiveness in terms of both time as well as security. As the information is used Cold-blooded algorithms enhance the security of encryption ways while also minimizing the time needed by algorithms that take a lengthy period to maintain security.

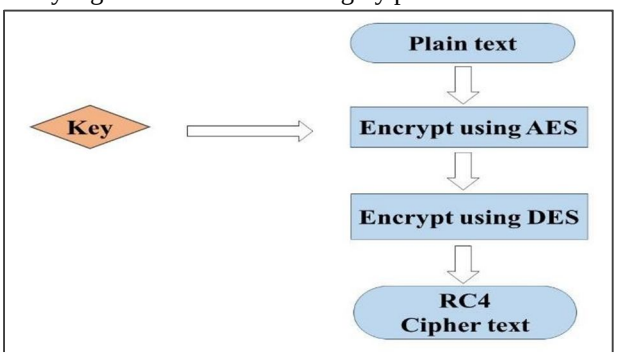


Fig. 1.Encryption phase of hybrid algorithm

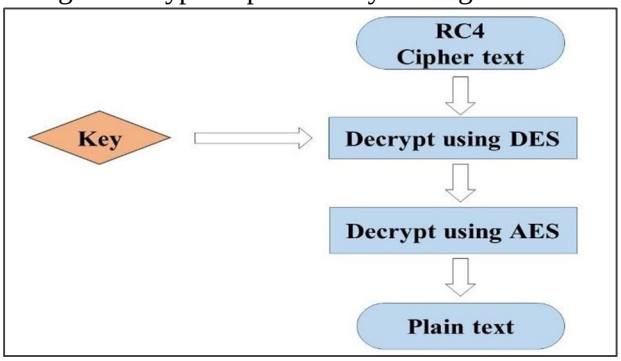


Fig.2 Decryption phase of hybrid algorithm system

In such cases, a hybrid encryption strategy is employed. The enormous amount of data is encrypted using the AES technique, and the AES key is encrypted using the DES algorithm in this methodology. The data cipher form is obtained by utilizing RC4 and an AES encrypted message and a DES-encrypted AES key. When the message is received, the AES key is first encrypted utilizing DES private key, and then the message is decrypted using the RC4 key. This hybrid encryption technique with java source code is demonstrated in figure 3. Encrypted and the decrypted text file are shown in figure 4 and figure 5 respectively. Figure 6 and figure 7 show Encrypted and decrypted image files respectively.

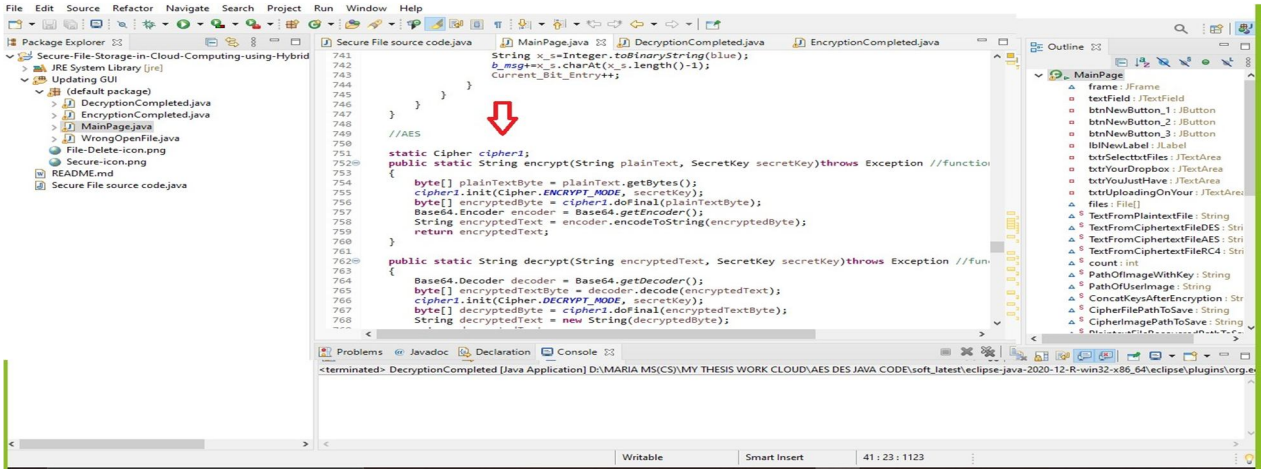


Fig. 3. Used source Code for hybrid System

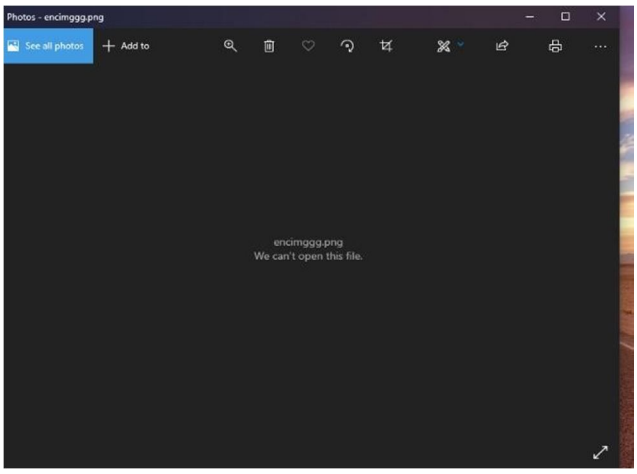


Fig. 6. Image in Encrypted form

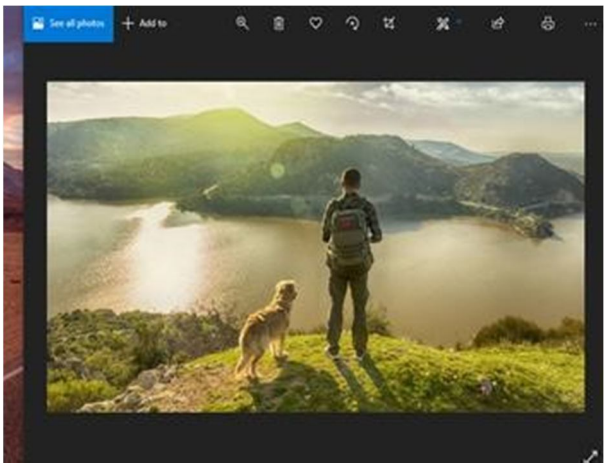


Fig. 7. Image in Decrypted form

Table 3. Factors for Configuration of different algorithms

Factors	DES	AES	RC4	Hybrid
Site of key	64bits	128,192,256 bits	256 bits	256 bits
flexibility	Scalable algorithm due to varying Block size	AES provides the high flexibility	RC4 provides the Scalability	More Scalable algorithm than another algorithm
Security	Secure for both user and provider	Secure Less than AES	Secure more than DES &AES	Provides high-level security
Data integrity protection on capacity	Provides security to small streams of data	Provide security to the small amount of data	Provide security to large streams of data	Fully developed security system for a large amount of data
Authentication mechanism	Provide Best authenticity	Less authentic than AES	Minimal Authentic	High-level authenticity
Memory utilization technique	Low RAM needed 14.8 KB	Needed RAM More than AES 18.3 KB	Needed RAM Less than AES & DES 16.6 KB	Low RAM needed 21.4KB
Algorithm type	Symmetric	Symmetric	Symmetric	Symmetric
Encryption level	Moderate	Faster	Faster	Faster
Decryption level	Moderate	Faster	Faster	Faster
Power Efficiency	Low	Low	Low	Low
Security	Not secured enough	Excellent Secured	Adequately secured	Highly secured
Key Usage	Encryption/decryption keys are the same.	Encryption/decryption keys are the same.	Encryption/decryption keys are the same.	Encryption/decryption keys are the same.

IV. RESULTS AND DISCUSSIONS

The studies are carried out on various sizes, using a hybrid of three algorithms: AES, RC4 as well as DES. The overall analysis of these algorithms is assessed using parameters like time for execution, and memory associated with implementation, also including the throughput.JAVA was being used to construct the established comparison model. The goal of the suggested hybrid cryptography method is to discover which of the previously described encryption techniques is the fastest and safest. So it allows the user to change the encryption algorithm that is most appropriate to the type of information they want to encrypt. The results demonstrate that the suggested hybrid system of algorithms increases the efficiency of encryption algorithms by securely encrypting data in a short amount of time. Table 3 shows the factors for algorithm configuration.

A. Analysis and Evaluation of the Hybrid System of Algorithm

1) Analysis And Evaluation Based On Encryption Time And Decryption Time

By assaying RC4 performs faster than DES and AES and a crossbred system of algorithms works multitudinous times fasters than all of the other algorithms. The creation of keys must be completed right before the encryption of data. This system is done in collaboration with both the user and the Pall service provider.

In comparison to former encryption algorithms, the crossbred system takes 10 to 15 lower time to reckon a train. Analogous data security can't be handed with a single encryption Fashion. The reverse of encryption time is known as decryption time, which is the calculated length of time it takes for the decryption algorithm to complete to produce an original text from a ciphertext. By assaying decryption time, the crossbred system of algorithms works well from all other algorithms. Figure 8 and figure 9 compare the encryption and decryption times of data ranging in size from 1 megabyte to 30 megabytes. Pearson correlation values in all couples are equal to 1 which demonstrates a strong positive relationship. P-A value of lower than0.05 shows the significance of the relationship and delicacy of data. Figure 8 and figure 9 show the Comparison of Encryption as well as decryption time of AES, DES, RC4, and Mongrel Algorithms.

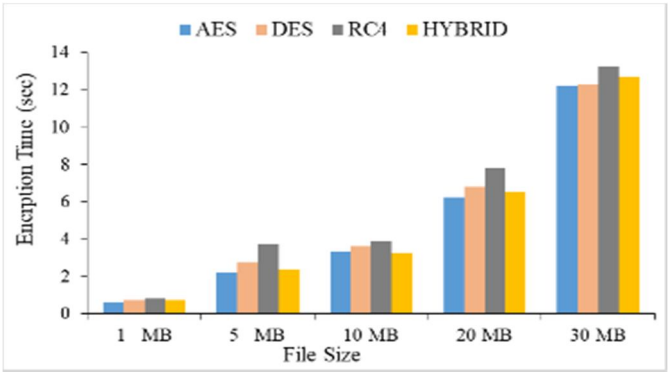


Fig.8 comparison of Encryption time of AES, DES, RC4, and Hybrid Algorithms

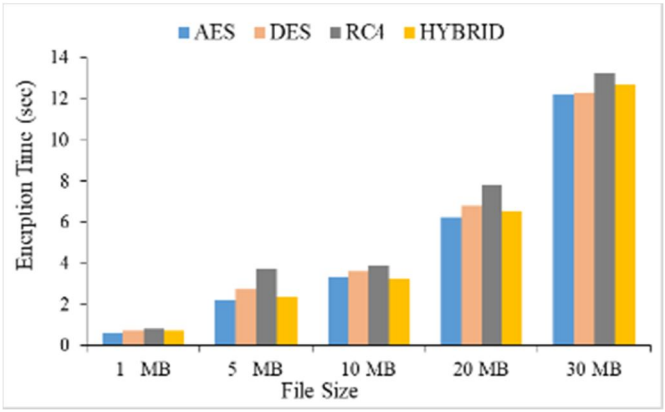


Fig.9 Comparison of Decryption time of AES, DES, RC4, and Hybrid Algorithms

2) Analysis And Evaluation Based On Memory Consumption

The amount of memory used during the encryption and decryption processes is referred to as memory utilization. RC4 consumes less memory than the DES and AES. The hybrid system of algorithms takes less memory consumption as compared to individual working of these three algorithms at the encryption/decryption time. Pearson correlation values in all pairs are equal to 1 which demonstrates a strong positive relationship. A P-Value of less than 0.05 shows the significance of the relationship and accuracy of the data. Figure 9 presented the Memory Consumption rate at the time of encryption and the memory consumption rate at the decryption time shown in figure 10.

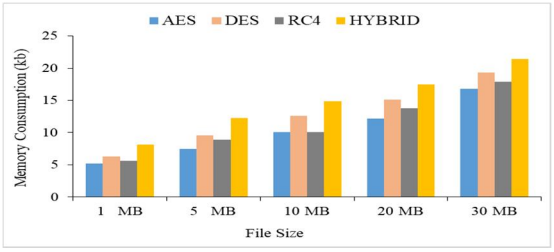


Fig. 9. Memory Consumption rate at the time of encryption

Fig. 10. Memory Consumption rate at the time of decryption

3) Analysis and evaluation based on Throughput calculation

At the encryption stage, the file size and the time it takes to complete encryption determine the throughput. This process is carried out for all file sizes.

Throughput = file size/encryption time …… (1)

At the decryption stage, overall throughput is estimated by measuring the file size by the time it takes to process decryption and then repeating the procedure for all file sizes.

Throughput = file size/decryption time……..….. (2)

The hybrid system of algorithms gives a good throughput rate as compared to the individual working of these three algorithms at the encryption and decryption time. When experiments are carried out at different file sizes such as 1MB, 5 MB, 10 MB, 20 MB, and 30 MB so the three systems AES, DES, and RC4 give less good throughput rate if takes the average of this throughput at encryption and decryption time on different file sizes as compared to a hybrid system of algorithms. Throughput rate shows at encryption/decryption time in Figures 11 and 12 respectively.

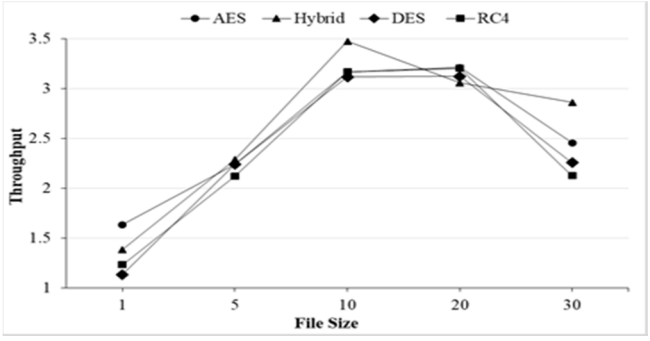


Fig. 11.Throughput comparison at the encryption stage

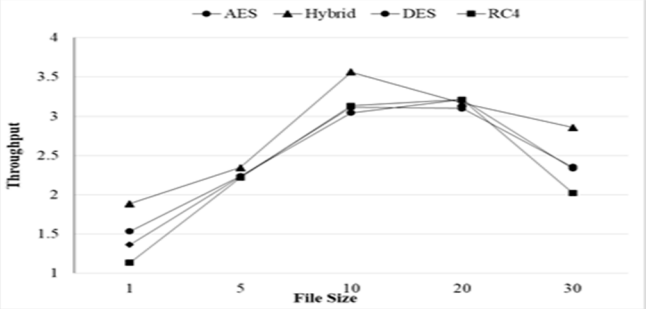


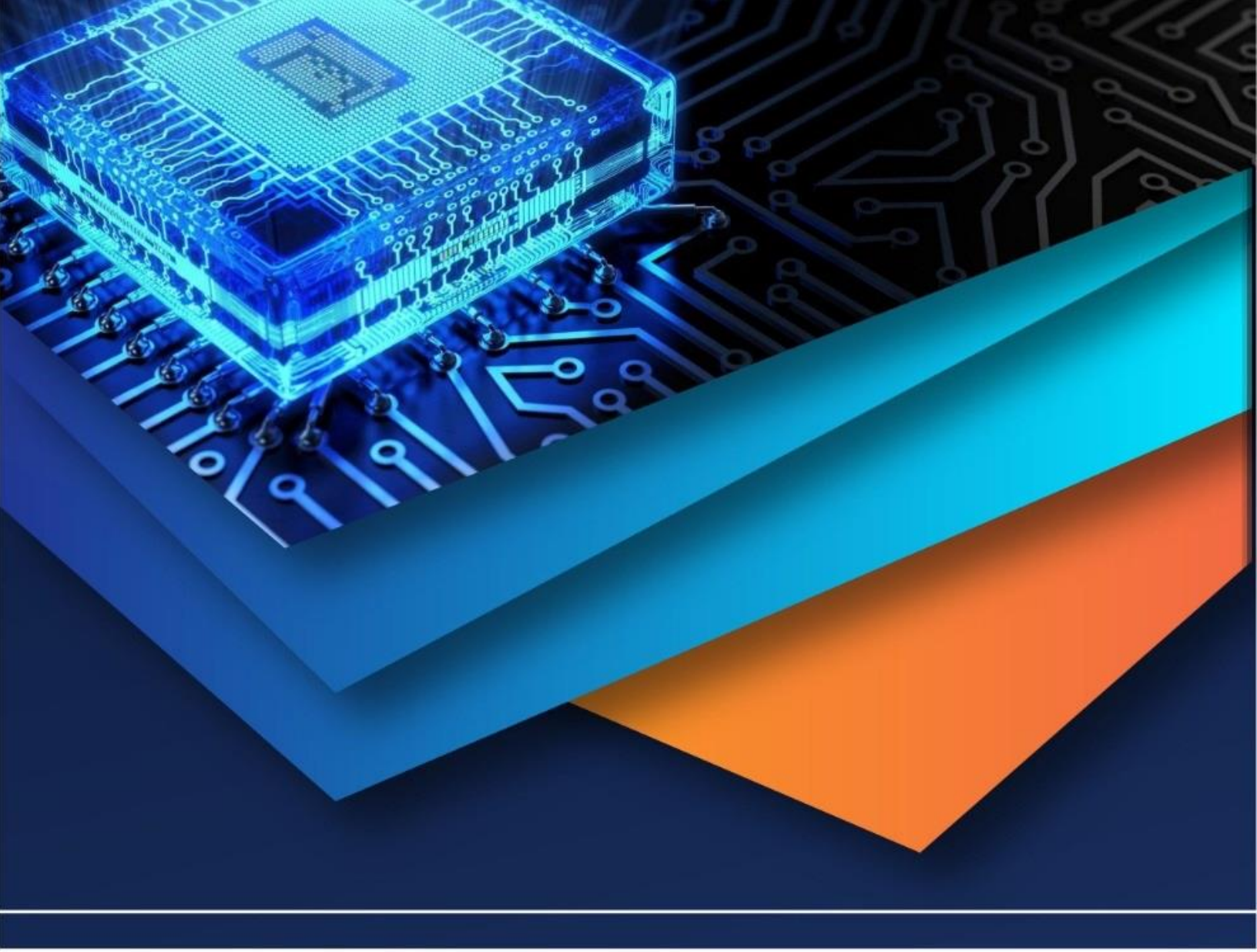
Fig. 12.Throughput comparison at the decryption stage

V. CONCLUSION

As the demand for cloud computing keeps growing, maintaining the integrity of the cloud as well as its users becomes a key priority. Several security methods may be used in the cloud. So here utilized a cryptography method to ensure the security of cloud storage. This hybrid method combines the cryptographic algorithms AES, DES, and RC4 to provide fast data security. The suggested technique is more efficient than existing techniques, according to analysis including its performance. In comparison to previous techniques, the methodology accomplishes hybrid encryption as well as decryption in a small amount of time. As a result, the suggested hybrid system of algorithms is beneficial for modern demands. This system creates random AES and DES keys & encrypts the accepted data file. The RC4 encryption technique is then used to encode the applied AES key. The AES key is encrypted, and the encrypted data file is concatenated and delivered via the communication medium. The merged file is approved on the receiver's side. The encrypted AES and DES key files and the encrypted data file are separated in this file. Data is decrypted using the AES and DES algorithms as well as RC4 keys. The goal of the hybrid algorithm system is to increase the level of security. Such a method can make it more difficult for the hacker to succeed. The required result for the data on cloud computing was accomplished by implementing a hybrid system of algorithms in the eclipse IDE tool using the Java language. In the future, various comparisons with other techniques for cryptography might be utilized to provide findings that demonstrate the efficiency of the suggested framework. As a result, more research will concentrate on improving encryption as well as decryption times. In addition, new hybrid algorithms should be built from existing methods to increase the encryption process as well as the level of security for cloud storage.

REFERENCES

[1] E. Ghazizadeh, "Cloud Surfing: A General Comparison of Cloud Identity Guidelines," in the proceedings of Americas Conference on Information Systems (AMCIS 2020), USA, pp. 30-34,2020.
[2] J. Gibson, "Benefits and challenges of three cloud computing service models." In the proceedings of Fourth International Conference on Computational Aspects of Social Networks (Cason), Brazil, pp. 198-205. 2012.
[3] A. Orobosade, "Cloud application security using hybrid encryption," Communications, vol. 7, pp. 25-31, 2020
[4] P. Srivastava, "A review paper on cloud computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 8, issue. 6. pp. 17-20, 2018.
[5] H. Tabrizchi, "A survey on security challenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, vol. 76, issue. 12. pp. 9493-9532, 2020.
[6] R. Chatterjee, "Cryptography in cloud computing: a basic approach to ensure security in the cloud," International Journal of Engineering Science, vol.7, issue. 5, pp. 11818-11821,2017.
[7] S. Sharma, "A hybrid cryptographic technique for file storage mechanism over the cloud," in First international conference on sustainable technologies for computational intelligence, Poland, Vol. 1045, pp. 241-256, 2020.
[8] K. Logunleko, "A comparative study of symmetric cryptography mechanism on DES, AES, and EB64 for information security," International Journal Scientific Research in Computer Science and Engineering, vol. 8, issue. 1. pp. 45-51, 2020.
[9] S. K. Ghosh, "Hybrid Cryptography Algorithm For Secure And Low-Cost Communication," in Proceedings of International Conference on Computer Science, Engineering and Applications (ICCSEA), UK, pp. 1-5, 2020.
[10] S. R. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, issue. 2. pp. 774-781, 2020.
[11] O. Hajihassani, "Fast AES implementation: A high-throughput bitsliced approach," IEEE Transactions on parallel and distributed systems, vol. 30, issue. 10. pp. 2211-2222, 2019.
[12] O. G. Abood, "A survey on cryptography algorithms," International Journal of Scientific and Research Publications, vol. 8, issue. 7. pp. 495-516, 2018.
[13] N. A. Sharma, "A performance test on symmetric encryption algorithms—RC2 Vs Rijndael," International Journal Of Scientific & Technology Research, vol. 6, issue. 07. pp. 292-294, 2017.
[14] K. Sajay, "Enhancing the security of cloud data using hybrid encryption algorithm," Journal of Ambient Intelligence and Humanized Computing, pp. 1-10, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY