iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43535

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 VI June 2022- Available at www.ijraset.com

Secure File Storage on Cloud Using Cryptography

Nandini K[1], Faisal. S[2], Shailendra B[3], Shree Vallabha S[4], Pavan B[5]
[1, 2, 3, 4, 5]*Department of Computer Science, Dayananda Sagar University, Bangalore, Karnataka*

Abstract: ***Hacking became a serious drawback lately. Transference of secure knowledge or communication through the web turns out to be difficult because of security considerations. to anticipate these security hurdles, we tend to use Cryptography, and Image Steganography. Day's cloud computing is currently employed in several areas like business, colleges, and Universities to store a great amount of knowledge. We will extract knowledge from the cloud for the asking of users. To store knowledge on the cloud we've to face several errors and issues. Cryptography and steganography techniques area unit well-liked currently a day's for knowledge security. using one algorithmic rule isn't effective for prime-level security to knowledge in cloud computing. during this paper, we initiated a new security mechanism using symmetrical key cryptography algorithmic rules and steganography. during this projected system AES, blowfish, RC6, and 3DES algorithms area units were used to supply block-wise security to knowledge. All algorithms have a key size of 128 bits. Key data contains that a part of the file is encrypted using that algorithmic rule and key. The file is split into eight components. every part of the file is encrypted using different algorithmic rules. All components of the file area unit are encrypted at the same time with the assistance of the multithreading technique. encoding Keys area unit inserted into cowl image using LSB technique. Steganography image is sent to a valid receiver using email. For file secret writing purposes reverse method of cryptography is applied.***

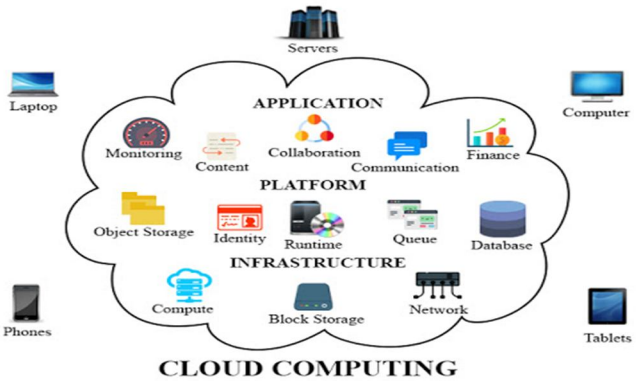
Keywords-Hacking, Steganography, Cryptography, Cloud service provider (CSP), cloud server (CS), Encode, Decode, Delay, Integrity

I. INTRODUCTION

Internet isn't any longer safe to transfer sensitive info. The dependence of the individuals created the hackers to observe the network and attack for sensitive info. the info is firmly saved in our system and won't be safe after we transfer it over the web. Also, the system itself may be established with viruses, trojans, and malware in the style ways that. This results in intrusion into the system and once more loss of data. Therefore, security is the most important factor for individuals since the evolution of hacking. Cryptography is the technique of embedding information into an object wherever human sense cannot sense it. This means the communication is accomplished in such how that the message's existence cannot be known. The word Cryptography in Greek may be shown as 'Krypto' suggests that it is hidden and 'graphene' suggests that writing. Security and protection keep a crucial obstruction on Distributed computing as an example safeguarding classification, uprightness, and accessibility of information. This methodology guarantees that the information is most certainly not noticeable to outer clients and cloud executives, however, has the impediment that plain content-based principally looking calculation does not appear to be relevant.

A. Cloud Computing

Cloud computing is the utilization of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Cloud computing entrusts remote services with a user's information, code, and computation. Cloud computing consists of hardware and code resources created and accessible online as managed third-party services. These services generally offer access to advanced code applications and high-end networks of server computers.



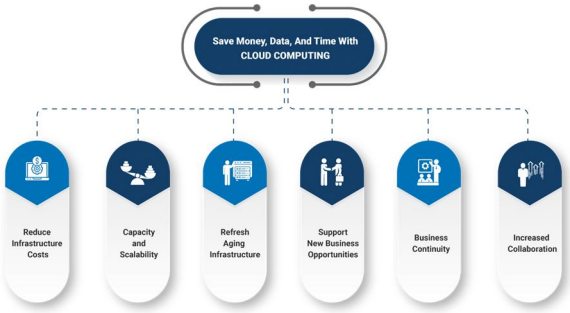
The goal of cloud computing is to apply traditional supercomputing, or superior computing power, ordinarily utilized by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications like financial portfolios, to deliver customized info, to produce information storage or to power giant, immersive laptop games. Cloud computing uses networks of huge teams of servers usually running low-priced shopper computer technology with specialized connections to unfold data-processing chores across them. This shared IT infrastructure contains massive pools of systems that are joined along. Often, virtualization techniques are accustomed to maximizing the power of cloud computing.

A. Benefits Of Cloud Computing

Achieve economies of scale – increase volume output or productivity with fewer individuals. Scale back payment on technology infrastructure. Maintain quick access to your info with nominal direct payment. Pay as you go (weekly, quarterly, or yearly), supported demand. widen your personnel on a budget. individuals worldwide will access the cloud, provided they need a web association. contour processes. Get additional work finished in less time with fewer individuals. scale back capital prices. There's no got to pay money on hardware, software, or licensing fees. Improve accessibility. you have got access anytime, anywhere, creating your life easier! The monitor comes additional effectively. keep among budget and sooner than completion cycle times. Less personnel coaching is required. It takes fewer people to try and do additional work on a cloud, with a nominal learning curve on hardware and software system problems. Minimize licensing new software systems. Stretch and grow while not the necessity to shop for overpriced computer code licenses or programs. Improve flexibility. you'll be able to modify direction while not serious "people" or "financial" problems at stake.

B. Advantages Of Cloud Computing

Pay for only the resources used. Cloud instances are isolated within the network from alternative instances for improved security. Instances are going to be value-added instantly for improved performance. Purchasers have access to the complete resources of the Cloud's core hardware. Auto-deploy cloud instances once required. Uses multiple servers for max redundancies. just in case of server failure, instances are going to be mechanically created on another server. able to log in from any location. Server snap and a package library allow you to deploy custom instances. Deals with a spike in traffic with fast preparation of further instances to handle the load.



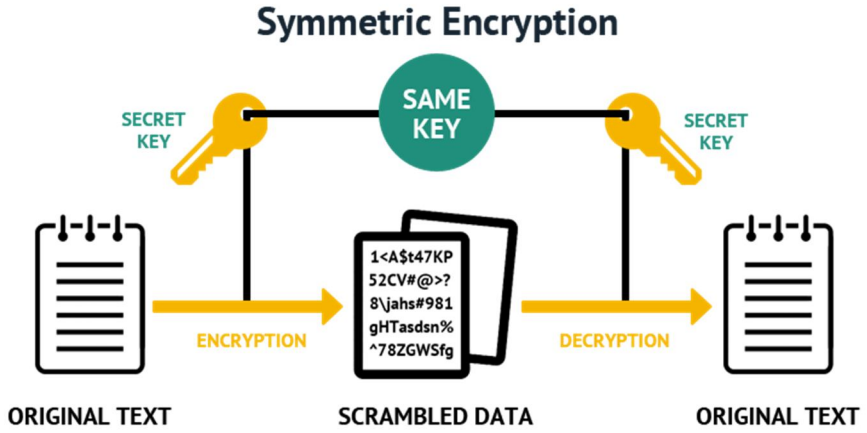
II. CRYPTOGRAPHY

Cryptography could be a methodology of protective info and communications through the utilization of codes so only those for whom the data is meant will scan and the method it. In technology, cryptography refers to secure info and communication techniques derived from mathematical ideas and a group of rule-based calculations known as algorithms, to rework messages in ways that are exhausting to decipher. These settled algorithms are used for cryptological key generation, digital signing, and verification to guard information privacy, internet browsing on the web, and confidential communications like MasterCard transactions and email. Cryptography is closely associated with the disciplines of cryptography and cryptology. It includes techniques like microdots, merging words with pictures, and alternative ways to cover info in storage or transit. However, in today's computer-centric world, cryptography is most frequently related to scrambling plaintext (ordinary text, generally named cleartext) into ciphertext (a method known as encryption), then back once more (known as decryption). people who observe this field are referred to as cryptographers.

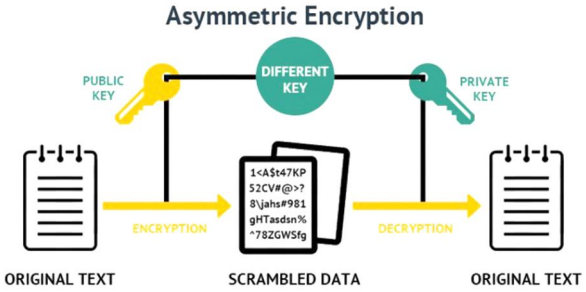
A. *Types Of Cryptography*

Cryptography is classed into two categories supported by the kinds of keys and cryptography algorithms:

1) *Symmetric Key Cryptography:* Also called Secret Key Cryptography, personal key encoding encrypts information providing a single key that only the sender and receiver understand. the secret key should be identified by each sender and therefore the receiver, however, shouldn't be sent across the channel; but, if the hacker obtains the key, deciphering the message is easier. once the sender and also the receiver meet on the telephone, the key should be addressed. though this can be not a perfect technique. as a result of the key remains constant, it's less complicated to deliver a message to a particular receiver. the info encoding framework (DES Algorithm) is the most generally used centrosymmetric key system.



2) *Asymmetric Key Cryptography:* Asymmetric key cryptography, additionally referred to as public-key cryptography, consists of two keys, a non-public key, that is used by the receiver, and a public key, that is declared to the general public. two completely different keys are utilized in this methodology to cipher and rewrite the information. These 2 distinct keys are mathematically connected. they're oversubscribed in pairs. the general public key's accessible to anyone, whereas the non-public key's only accessible to the one that generates these two keys.



III. OBJECTIVE

The proposed paper meets the desired security desires and implementation of the info center of the cloud server. The paper uses some regular key cryptography techniques in addition to stenography techniques. the concept of splitting and merging adds on to satisfy the principle of knowledge security. This hybrid approach once enforced during a cloud server makes the remote server safer and so, helps the cloud suppliers to do their work additional firmly. For knowledge security and privacy protection issues, the basic challenge of separation of sensitive data and access management is fulfilled. The Cryptography technique converts original information into ciphertext. The cryptography technique is split into symmetric-key cryptography and public-key cryptography. therefore only an authorized person will access data from the cloud server. Ciphertext data is visible to all people. but for that again the cryptography technique needs to be used to translate it back into the initial text.

IV. RELATED WORK

1) They focused on the information over-collection drawback. They tried to place all client details into a cloud the security of client details might be multiplied they have explored numerous experiments and also the output shows the effectiveness of their approach. Their most direct improvement was reducing the storage in client smartphone footage, videos and different storage info or information occupy a lot of space for storing therefore these are vacated that alter users to put in new applications. They showcased an active approach. Whenever an application needs client information it has to access requests within the cloud.
2) Attribute-based proxy re-encryption scheme (ABPRE) may be a new science primitive that extends the normal proxy re-encryption (public key or identity-based cryptosystem) to the attribute-based counterpart, and so empower users with delegation capability within the access management surroundings. Users, known by attributes, might freely designate a proxy that will re-encrypt a ciphertext connected with an exact access policy to another one with a different access policy. The planned scheme is proven selective-structure chosen plaintext secure and passkey secure without random oracles. Besides, we tend to develop another quite key authorization capability in our theme and additionally discuss some connected problems together with a stronger security model and applications.
3) In the security model symmetric algorithm uses chunk level encryption and decryption of data in cloud computing. The key size is 256 bit. The Key is rotated to achieve high-level security. For data integrity purposes hash value is generated. Hash values are garnetted after encryption and before decryption. If both hash values match then that data is in the correct form. In this security model, only valid users can access data from the cloud. The advantages of the security model are integrity, security, and confidentiality.
4) Three algorithms are used for the implementation of the hybrid algorithm. For user authentication purposes a digital signature is used. The blowfish algorithm is used to produce high data confidentiality. It is an asymmetric algorithm. It uses a single key. The blowfish algorithm needs the least amount of time to encode and decode. The subkey array concept is used in the blowfish algorithm. It is a block-level encryption algorithm. The main aim of this hybrid algorithm is to achieve high security for data for upload and download from the cloud. A hybrid algorithm solves the security, confidentiality, and authentication issues of the cloud.

V. SYSTEM DESIGN

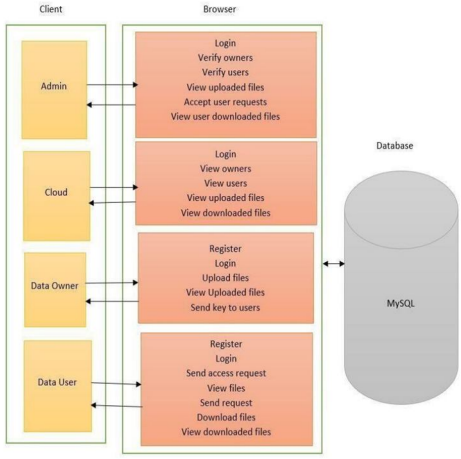
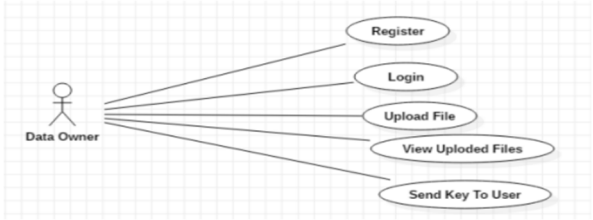


Fig 1. Project Design

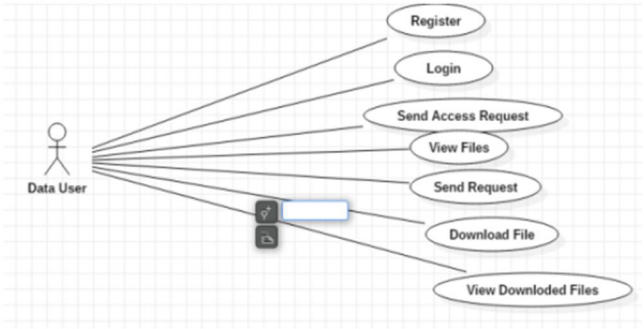
We propose a method that provides high security. The user uploads a file into the cloud which has public and private fragments. The private fragment is supposed to be securely protected. As said before we have proposed to use the Double Encryption Technique. For Double Encryption, the algorithms that we have used are AES,3DES, and Blowfish. Here we first encrypt the private fragment containing the important information with AES128. After the first encryption is over the corresponding key is generated. This encrypted file is again subjected to encryption with another algorithm.

Fig1.1 Data owner Use case diagram.



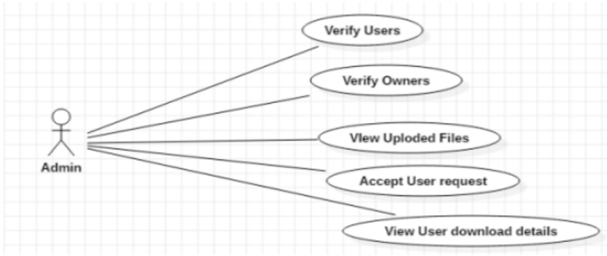
Data Owner needs to register first and through the login, the owner of the details needs to upload the file after uploading the file owner can send the key to the user.

Fig1.2 Data User Use case diagram



Data User will have to register and login through those given credentials and send an access request to the owner to view those files and then through the given key user can download the file.

Fig1.3 Admin use case diagram



Admin has to verify the user and owner after verifying admin can view uploaded files and has permission to accept user requests and can also view user download details.

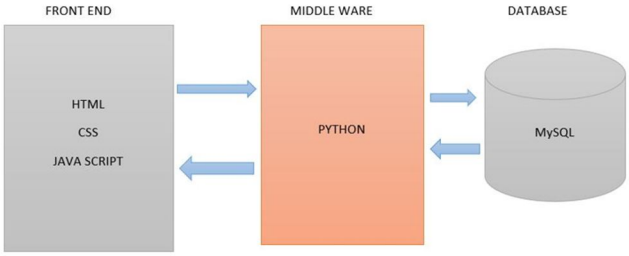


Fig 2. Technical Architecture

VI. PROPOSED SYSTEM

Algorithm

1) Start
2) Admin will be managing all the system operations.
3) Cloud Admin will just see the members, uploaded files, and downloaded files.
4) Data Owner will upload the file which is encrypted with double encryption using (AES, Blowfish & Triple DES) algorithms. The first encryption will be done by using AES the and second encryption will be done using Blowfish & triple DES based on the size of the file.
5) After that the file is divided into 7 fragments and will be saved in a real-time cloud (Firebase)
6) Data User will not able to see any files after he login then data user will request to see the files then the admin will request, when he accepts data user will see the files but not able to see the information in them.
7) Data User will keep request to file then the request is sent to data owner who is uploaded the file if the data owner accepts the request and send the keys to the data use.
8) The keys sent by the data owners are not original keys, the keys are like OTP(one-time-password) used by the particular user and a particular time.
9) Then data user can download the file by using that keys.
10) end

VII. IMPLEMENTATION

The system has been implemented using AES,3DES, and Blowfish algorithms. The algorithms are explained here.

A. Working on AES Algorithm

1) Obtain the key from the cipher key.
2) Assign the plain text to the state array.
3) Prefix state array with initial round key.
4) Perform manipulation nine times.
5) Carry out the tenth and last manipulation.
6) Copy ciphertext.

Figure 3 represents the working of the AES algorithm. AES is an iterative cipher. It is symmetrical block cipher algorithm. It is capable of encrypting 128 bits of plain text. The various keys used by this algorithm are 128,192,256 bits. It is considered the most secured algorithm

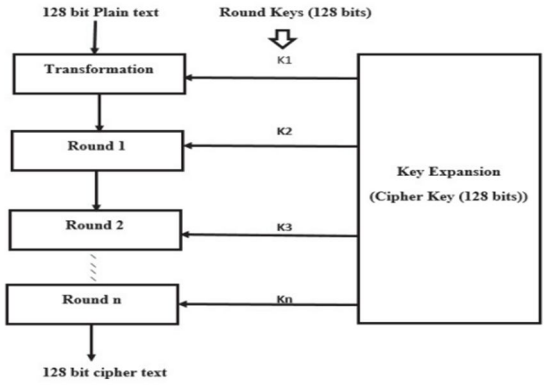


Fig. 3. Working of AES Algorithm

B. Working on 3DES Algorithm

1) Encrypt the plaintext blocks using a single DES with key K1.
2) Now decrypt the output of step 1 using a single DES with key K2.
3) Finally, encrypt the output of step 2 using a single DES with key K3.
4) The output of step 3 is the ciphertext.
5) Decryption of a ciphertext is a reverse process. The user first decrypts using K3, then encrypt with K2, and finally decrypts with K1.

Due to this style of Triple-DES as encrypt–decrypt–encrypt method, it's potential to use a 3TDES (hardware) implementation for one DES by setting K1, K2, and K3 to be identical to the same. This provides backward compatibility with DES. Triple DES systems area unit considerably safer than single DES, however, these are clearly a way slower method than encoding exploitation single DES.

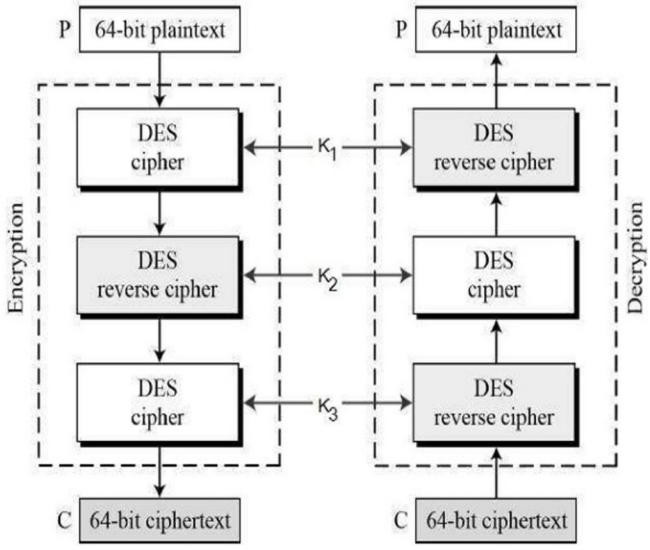


Fig.4 Working of 3DES Algorithm

C. Working on Blowfish Algorithm:

1) Generation of subkeys: 18 subkeys{P[0]…P[17]} are needed in both encryption as well as decryption process and the same subkeys are used for both the processes. These 18 subkeys are stored in a P-array with each array element being a 32-bit entry.
2) 4 Substitution boxes(S-boxes) are needed:{S[0]…S[4]} in both encryption aswell as decryption process with each S-box having 256 entries{S[i][0]…S[i][255], 0&lei&le4} where each entry is 32-bit.

3) Encryption

The encryption function consists of two parts:

a) *Rounds:* The encryption consists of 16 rounds with each round (Ri) taking inputs from the plaintext (P.T.) from the previous round and the corresponding subkey (Pi).

b) *Post-processing:* The output after the 16 rounds is processed.

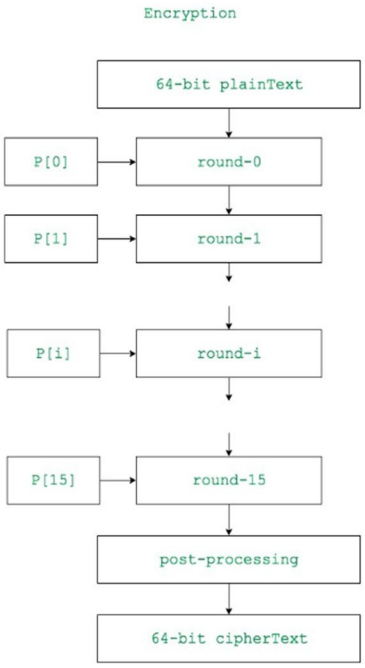


Fig 5. Working of Blowfish Algorithm

TABLE I. DATA TABLE FOR ENCRYPTION RUNTIME OF TEXT FILE

File(MB)	DES (in sec)	Blowfish (in sec)	RC5 (in sec)	3-DES (in sec)	AES+RSA (in sec)
0.1	2.5	1.2	1.5	2	1
0.5	3	1.6	1.8	2.5	1.5
0.75	4.5	4	4.2	4.5	3.5
1	5.5	4.5	4.8	5	4
Average time	15.5	11.3	13.8	14	10
Throughput(MB/sec)	1	1.8	1.6	1.25	2

TABLE II. DATA TABLE FOR DECRYPTION RUNTIME OF TEXT FILE

File(MB)	DES (in sec)	Blowfish (in sec)	RC5 (in sec)	4-DES 5-(in sec)	AES+RSA (in sec)
0.1	2.0	1.2	1.5	1.8	1
0.5	2.5	1.8	2	2.3	1.5
0.75	3	2.3	2.5	2.7	2
1.0	4	3.5	3.5	3.8	3
Average time	11.5	8.8	9.5	10.6	7.5

VIII. IMPLEMENTATION AND RESULT

We have created a web-based application to give access to the authorized users of the application to communicate and transfer the data among themselves.

Fig.6 Owner Registration Form where the user needs to fill up the details of the form and then for verification, he needs to add an image as a captcha.

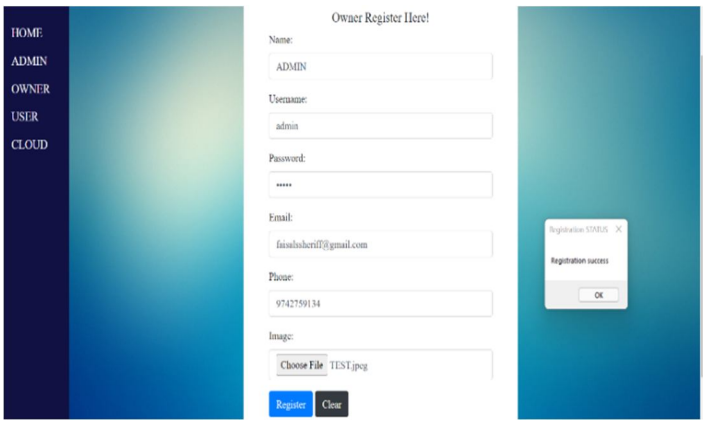


Fig.6 Owner Registration Form

Fig 7. User Registration Form where the user needs to fill up the details of the form and then for verification, he needs to add an image as a captcha.

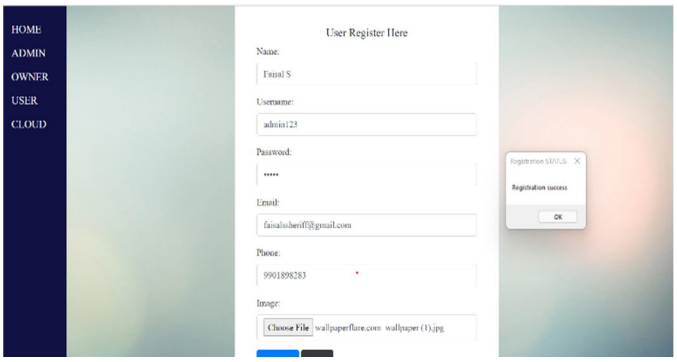


Fig.7 User Registration Form

Fig.8 Admin Verifying User after the user registration process the id and status would be visible to the admin then can activate the credentials.

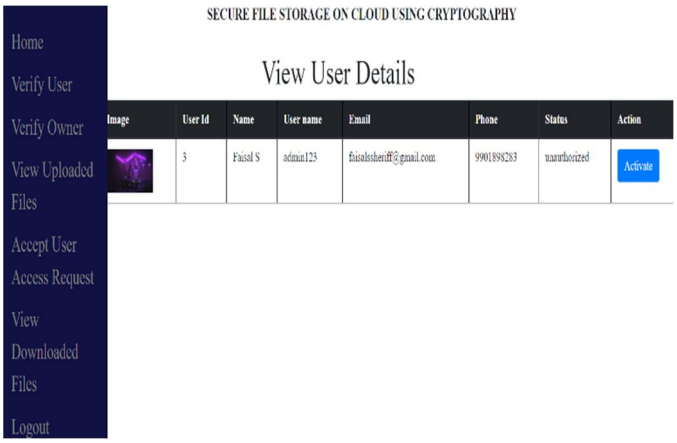


Fig.8 Admin Verifying User

Fig.9 Owner Uploading File where user can fill up filename and description then the owner needs to upload file in the cloud.

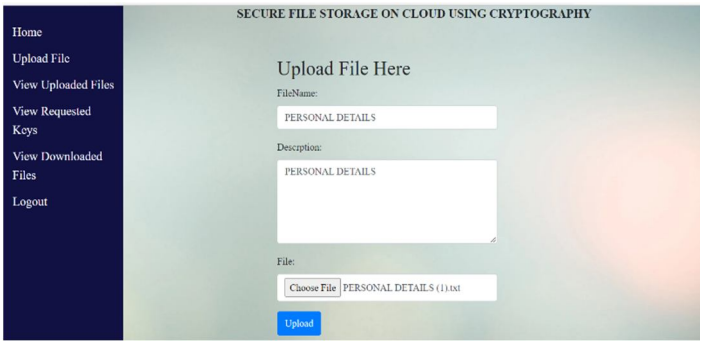


Fig.9 Owner Uploading File

Fig.10 File Uploaded in Fragments as the process of uploading text files then through the 3DES algorithm the text is split into fragments and uploaded to the cloud later can be retrieved by the user after the owner's acceptance.

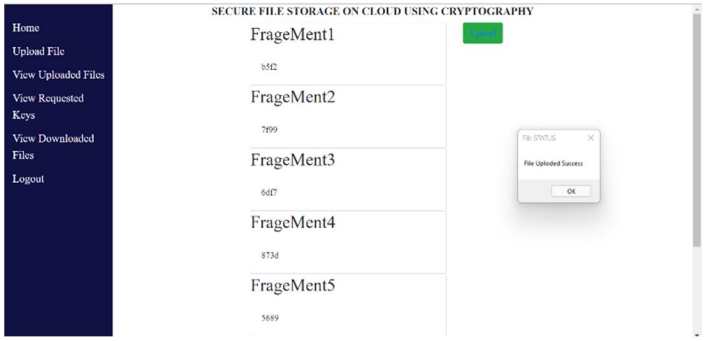


Fig.10 File Uploaded in Fragments

Fig.11 User-key request activation response page after the process of the fragments break down the user gets the key for downloading decrypted data into useful information.

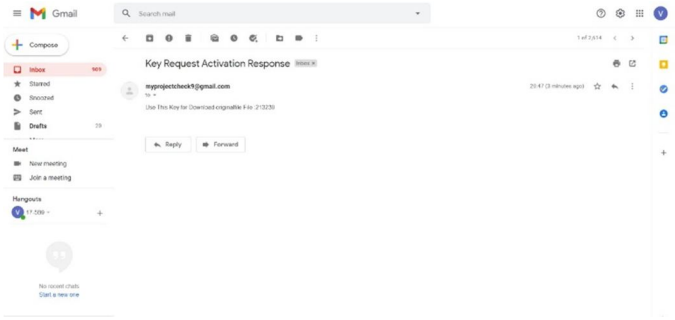


Fig.11 User-key request activation

Fig.12 User-key verification page to download the given data using the user-key which has been sent to mail id.

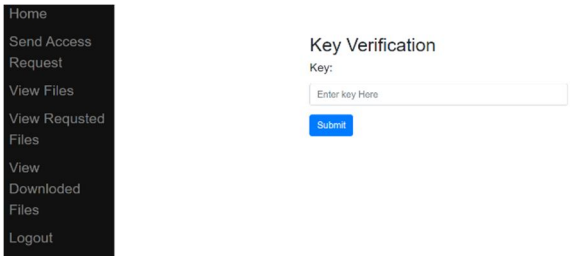


Fig.12 User-key verification page to download

Fig13.User-requested file details page through the activation key he can download the file using this link and then he download the data.

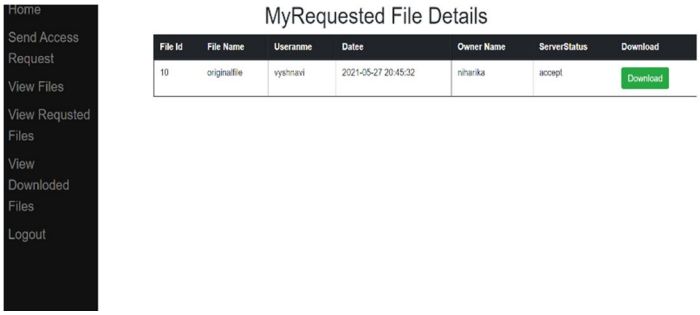


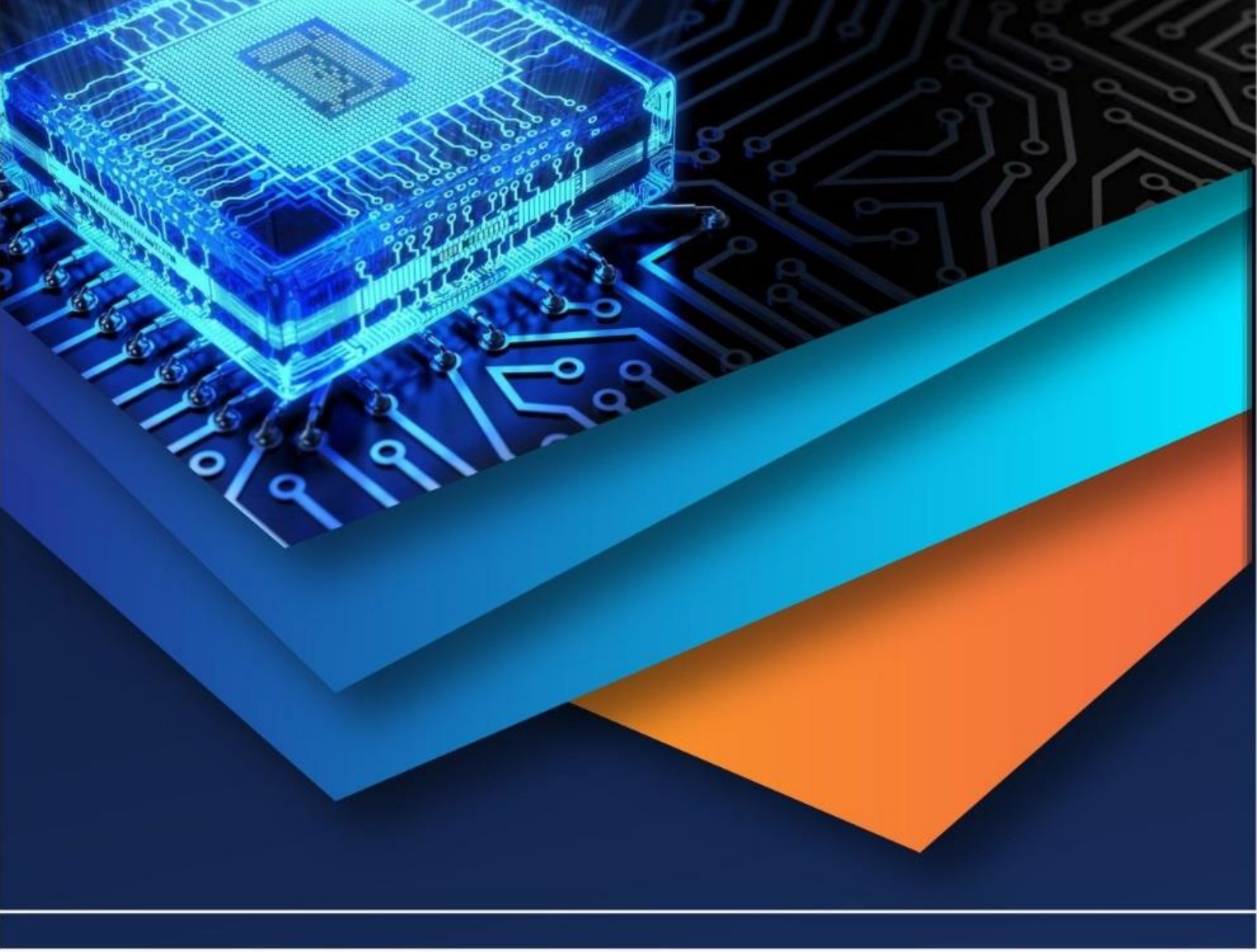
Fig13.User-requested file.

IX. CONCLUSION

In this paper, we tend to propose a way to supply high information security whereas using Cloud storage services. we build use of the Double cryptography Technique to extend the protection of the file. From the results obtained, our technique provides high security with resistance against propagation errors. The runtime of our algorithmic rule is less compared to the present algorithms, thus it's quick. Therefore, we tend to propose a secure and price-effective information protection technique for cloud service end-users. Our system efficiency in terms of runtime with secure protection of text information over the cloud compared with existing cryptography and decryption methodologies like AES, Blowfish, and 3DES. Our proposed conspire establishes a framework for future characteristic based, secure information for the executives and savvy contract improvement. As a future enhancement, we can accomplish high-level security using the hybridization of public-key cryptography algorithms.

REFERENCES

[1] Fuhry, B., Hirschoff, L., Koesnadi, S., & Kerschbaum, F. (2020). SeGShare: Secure Group File Sharing in the Cloud using Enclaves. 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). doi:10.1109/dsn48063.2020.00061
[2] Inder Singh, M. Prateek," "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma, A. Hasan, "A New Method Towards Encryption Schemes, IEEE, International Conference on Reliability, Optimization and Information Technology, pages 310-313, Feb 2019.
[3] Jasleen K., S.Garg, "Security in Cloud Computing using Hybrid of Algorithms", IJERJS, Volume 3, Issue 5, ISSN 2091-2730, pages 300-305, September-October, 2015
[4] Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021). Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI). doi:10.1109/esci50559.2021.9397005
[5] Pronika, & Tyagi, S. S. (2021). Secure Data Storage in Cloud using Encryption Algorithm. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). doi:10.1109/icicv50876.2021.9388388
[6] Subasini, C. A., & Nikkath Bushra, S. (2021). Securing of Cloud Data with Duplex Data Encryption Algorithm. 2021 5th International Conference on ComputingMethodologiesandCommunication.(ICCMC). doi:10.1109/iccmc51019.2021.9418
[7] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021). Cloud Security using Hybrid Cryptography Algorithms. 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). doi:10.1109/iciem51511.2021.94453
[8] Kodumru, N. L., & Supriya, M. (2018). Secure Data Storage in Cloud Using Cryptographic Algorithms. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). doi:10.1109/iccubea.2018.8697550



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY