SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

Khumani[1], Priya Roy[2], Swapnil[3], Suman Madan[4]

[1,2,3]*Research Scholar, Jagan Institute of Management Studies, Sector-5, Rohini, Delhi, India.*

[4]*Associate Professor, Jagan Institute of Management Studies, Sector-5, Rohini, Delhi, India*

Article DOI: https://doi.org/10.36713/epra8447
DOI No: 10.36713/epra8447

ABSTRACT

In this paper our intention is to soundly preserve records into the cloud, with the aid of the usage of splitting statistics into numerous chunks and storing components of it on cloud with inside the route of a way that preserves statistics confidentiality, guarantees availability and integrity. The all at once superior use of cloud computing with inside the various corporation and IT industries offers new software program with low fee. Cloud computing is beneficial in phrases of low fee and accessibility of records. Cloud computing offers lot of blessings with low fee and of records accessibility via Internet. Ensuring the protection of cloud computing can be a outstanding take into account the cloud computing environment, as customers regularly preserve touchy records with cloud garage corporations, however the ones corporations additionally may be untrusted. So, sharing statistics in normal way at the same time as keeping statistics from an untrusted cloud stays a tough issue. Our method guarantees the protection and privateness of consumer touchy records with the aid of the usage of storing statistics at some point of unmarried cloud, with the use of AES, DES and RC2 sets.

KEYWORDS— ***Cloud computing, Data Security, Cryptography, Storage.***

I. INTRODUCTION

It is originated from in advance large-scale allotted computing era. NIST defines Cloud computing as a version for permitting convenient, on call for community get proper of access to a shared pool of configurable computing re-assets (for example: networks, garage, applications and offerings) so one may be all at once provisioned and launched with agency issuer interaction or minimum control attempt[1].

In Cloud computing, each documents and software program software are not honestly contained at the purchaser computer. File safety issues stand up due to the reality each purchaser software program and software program software are residing in issuer premises. The cloud issuer can solve this problem with the aid of the usage of encrypting the documents with the aid of the usage of the use of encryption set of recommendations [2].

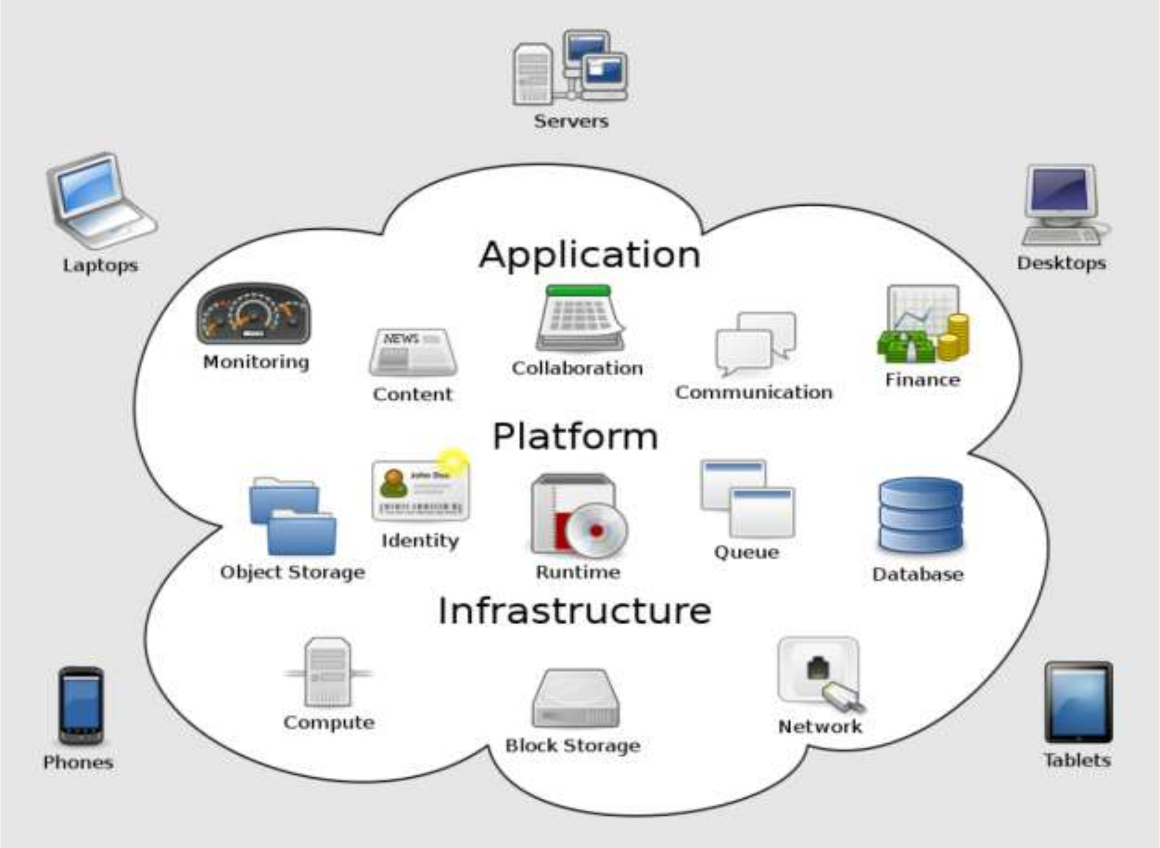


Figure 1: Structure of Cloud Computing

Cryptography is associated with the approach of changing regular easy textual content into unintelligible textual content and vice-versa. It is a manner of storing and transmitting statistics with inside the route of a selected shape certainly so simplest the ones for whom it is supposed can examine and test. Cryptography now no longer simplest protects statistics from robbery or alteration, however furthermore may be used for purchaser authentication. Cryptography with inside the cloud employs encryption strategies to normal statistics so one may be used or saved with inside the cloud. It allows customers to without troubles and securely get proper of access to shared cloud offerings, as any statistics it absolutely is hosted with the aid of the usage of cloud corporations is covered with encryption technique.

This paper offers a record safety version to deliver a green answer for the crucial problem of safety in cloud environment. In this version, hybrid encryption is used in which documents are encrypted with the aid of the usage of blowfish coupled with record splitting and SRNN (changed RSA) is used for the secured conversation among customers and the servers.

II. RELATED WORK

A literature evaluation is a motive essential precis of posted studies literature applicable to a subject below hobby for studies. Ten posted articles are referred so you could make an enterprise company base approximately the project. Following is a quick evaluation of all of the ten papers which have been referred: - Secure record garage in cloud the use of Hybrid Cryptography [3]. Punam V. Maitri, Aruna Verma, Year “2016 makes a strong point of methods documents may be securely saved on cloud. It discusses the problem with the use of an unmarried set of recommendations to encrypt the record and the way useless it is going to be on cloud. The approach mentioned in paper splits record into blocks and every block is encrypted the use of AES, BRA, blowfish, RC6 algorithms. The key records and records approximately which record makes use of which set of recommendations is despatched to the receiver the use of Steganography. Modern method to record device integrity checking [4].

M. Malarvizhi, J. Angela Jennifar Sujaana, T.Revathi, (2014) described “The important recognition of the paper is on integrity of documents and restoring the documents if integrity is breached. The proposed device makes use of sample of every covered record to decide its modification. Method used for sample era are cryptographic hash functions.

The device makes use of a database which shops the names of documents that require to be covered and their hash codes. To take a look at the integrity of the record the hash code of the record is produced and checked with one withinside the database. If the record is installation in reality then get proper of access to is granted in any other case the administrator is alerted and if a stored replica is to be had of the equal record, then the record is restored. New method to purchaser authentication the use of virtual signature [5].

Jerzy Kaczmarek, MichaÅ, WrÃbel, described a manner to integrity of documents and restoring the documents if integrity is affected. The proposed device makes use of sample of every covered record to decide its modification. Methods used for sample era are cryptographic hash function. The device makes use of a database which shops the names of documents that require to be covered and their hash codes. To take a look at the integrity of the record the hash code of the record is produced and checked with one withinside the database. If the record is installation in reality then get proper of access to is granted in any other case the administrator is alerted and if a stored replica is to be had of the equal record, then the record is restored. Secure record sharing the use of cryptographic strategies in cloud [6]. Rashi Dhagat, Purvi Joshi, made a strong point of providing the ability to soundly preserve and percentage the statistics in a selected corporation the use of clouds for garage. The approach proposed with withinside the paper makes use of corporation signature and encryption strategies. The blessings of the approach proposed is that statistics proprietors can preserve the record without revealing their identification to others withinside the cloud. Public key extrude scheme it absolutely is addressable (PKA) [7]. Bilal Habib, Bertrand Cambou, Duane Booher, Christopher Philabaum offered a brand-new approach to place into impact public key infrastructure. The PKI has the disadvantage that the relation among public and private key is maintained. Paper proposes a opportunity PKI scheme with addressable elements **(PKA)**.

III. PROPOSED WORK

In the proposed device, a way for securely storing documents within the cloud the use of a hybrid cryptography set of recommendations is presented, as shown in figure 2. In this device, the purchaser can maintain the report successfully in online cloud garage as those documents can be saved in encrypted shape withinside the cloud and pleasant the crook purchaser has gotten get right of entry to their documents.

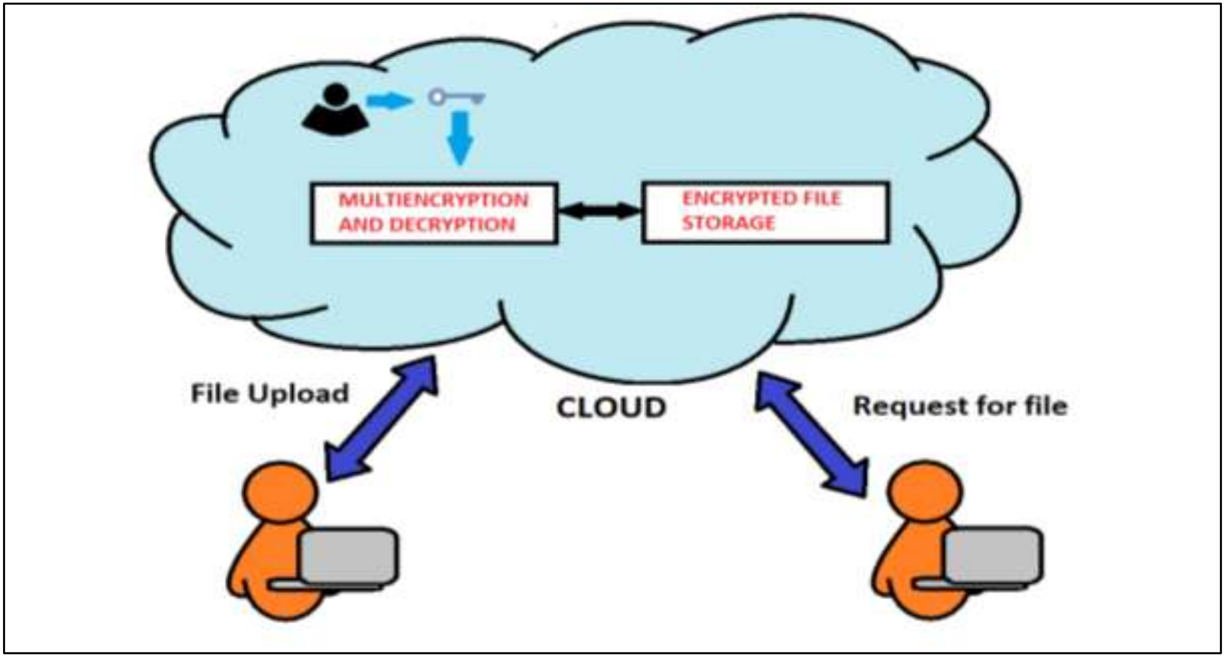


Figure 2: System Overview

The above determine offers an outline of the device. As withinside the above determine, the documents that the purchaser will add at the cloud can be encrypted with a purchaser-unique key and maintain successfully at the clouds.

1. **User Registration:** For having access to the offerings the purchaser need to first sign up yourselves. During the registration machine several records like Name, username, password, e-mail id, and the tele-call smartphone sizable variety can be asked to enter. Using this records the server will produce unique purchaser-unique keys that lets in you for use for the encryption and

decryption motive. But this key will now no longer be saved withinside the database as an alternative it'll in all likelihood be saved the use of the steganography set of recommendations in a photograph that lets in you for use because of the truth the purchaser's profile photograph.

2. **Uploading a File on Cloud :** Steps are:
   - When the purchaser uploads a report at the cloud first it'll in all likelihood be uploaded in a short folder.
   - Then purchaser's report can be cut up into N components.
   - These all components of report can be encrypted the use of cryptographic algorithms. Every element will use a selected encryption set of recommendations.
   - These all components of report can be encrypted the use of specific algorithms which might be AES, 3DES, RC6.The key to those algorithms can be retrieved from the steganographic photograph created withinside the route of the registration.
   - After the cut up encryption, the report reassembled and saved withinside the purchaser's unique folder. The genuine report is eliminated from the short folder.
   - Then Combining all Encrypted Parts of report.

3. **Download a File from the Cloud :** Steps are:
   - When the purchaser requests a report to be downloaded first the report is cut up into N components.
   - Then those components of report can be decrypted the use of the same algorithms with which they had been encrypted. The key to the algorithms for the decryption machine can be retrieved from the steganographic photograph created withinside the route of the registration.
   - Then those components can be re-mixed to shape a totally decrypted report

IV. SECURITY

The hybrid cryptosystem used to maintain security of the files has two phase: Encryption Phase and Decryption Phase. This section explains these phases:

1. **Encryption Phase:** At the encryption end,
   - On the specification of patron, the file being encrypted may be sliced into n slices. Each of the file slices is encrypted the usage of Blowfish key provided with the resource of the use of the patron for each slice, as shown in figure 3.
   - The key may be encrypted the usage of RSA public key
   - After encryption, we have got were given encrypted files slices and the corresponding encrypted keys. The process is shown in figure 4.

2. **Decryption Phase:** At the decryption end,
   - The patron will provide n RSA non-public keys, constant with the amount of slices (n) created with inside the direction of encryption phase. Blowfish key is decrypted at the server surrender the usage of the RSA non-public key specific to the slice, as shown in figure 5.
   - Using corresponding decrypted Blowfish keys, file slices stored in server are decrypted.
   - The decrypted slices may be merged to generate specific file.

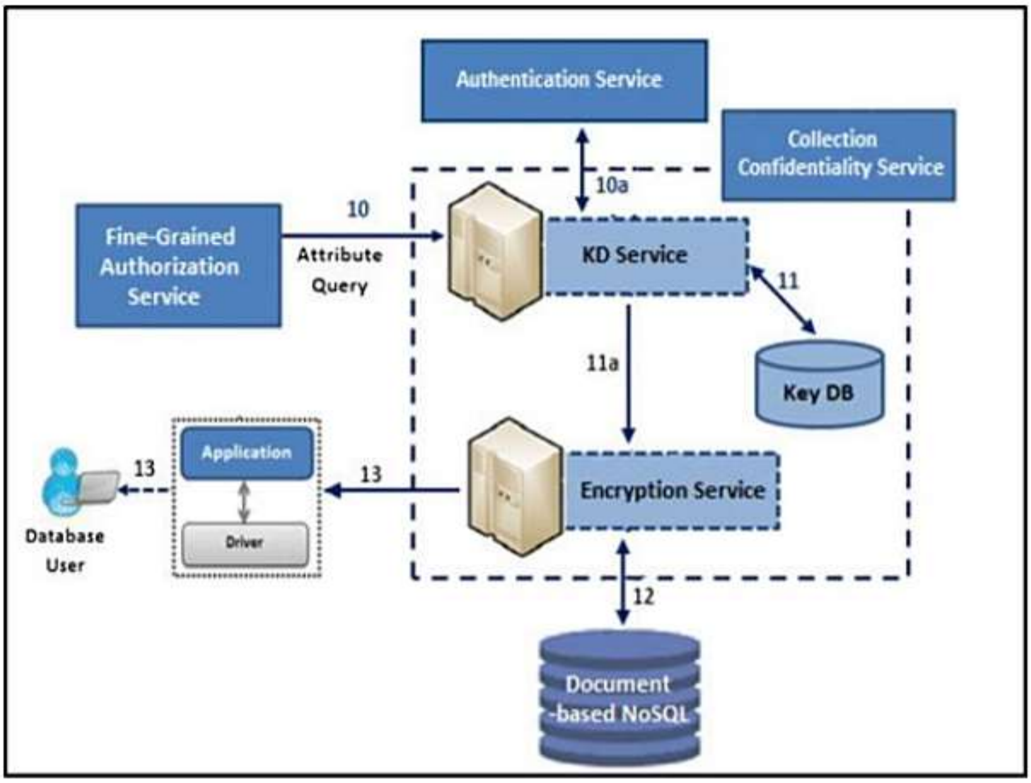


Figure 3: Ki - BlowFish Key

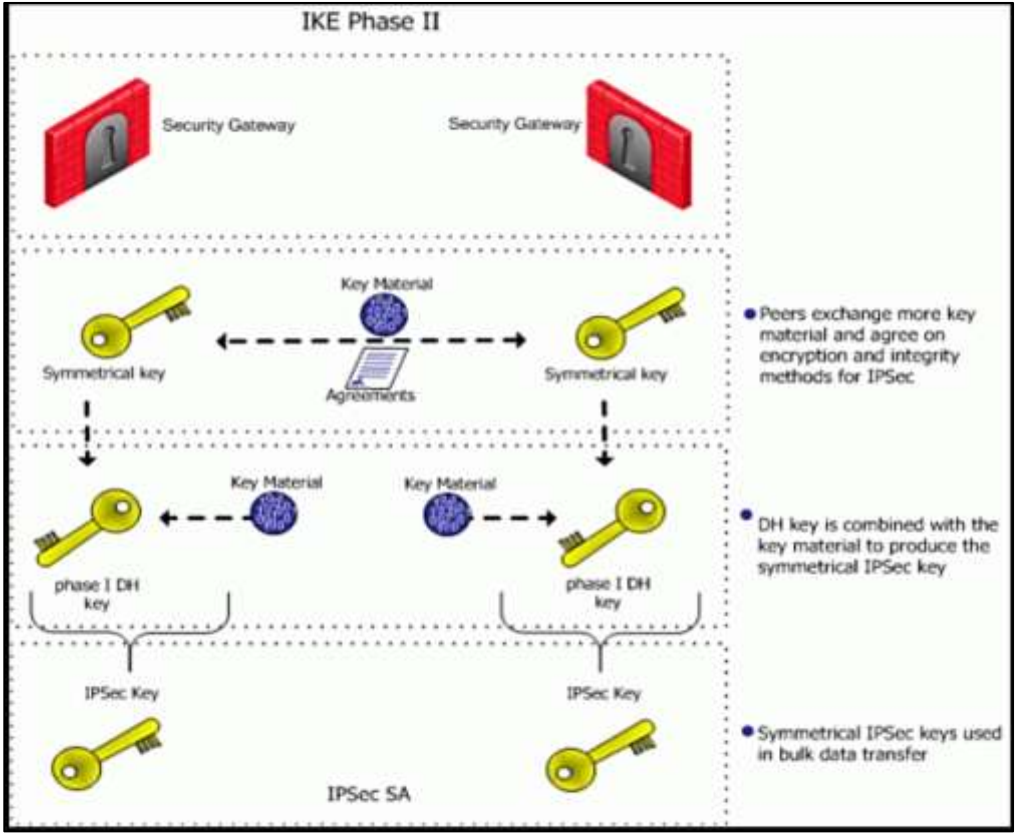

IKE Phase II
Security Gateway
Security Gateway
Key Material
Symmetrical key
Agreements
Symmetrical key
Peers exchange more key material and agree on encryption and integrity methods for IPSec
Key Material
Key Material
phase I DH key
phase I DH key
DH key is combined with the key material to produce the symmetrical IPSec key
IPSec Key
IPSec Key
Symmetrical IPSec keys used in bulk data transfer
IPSec SA

Figure 4: Eki – Encrypted BlowFish Key

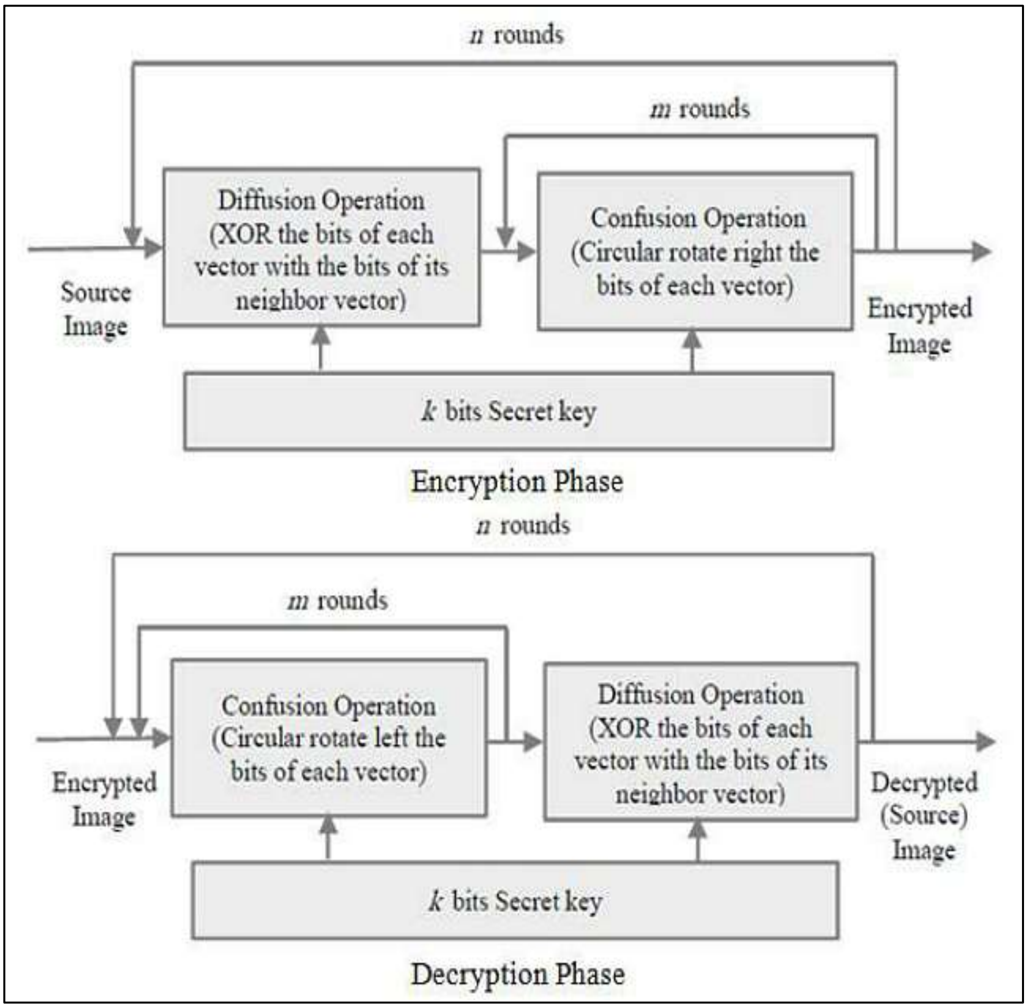

n rounds
m rounds
Source Image
Diffusion Operation (XOR the bits of each vector with the bits of its neighbor vector)
Confusion Operation (Circular rotate right the bits of each vector)
Encrypted Image
k bits Secret key
Encryption Phase
n rounds
m rounds
Encrypted Image
Confusion Operation (Circular rotate left the bits of each vector)
Diffusion Operation (XOR the bits of each vector with the bits of its neighbor vector)
Decrypted (Source) Image
k bits Secret key
Decryption Phase

Figure 5: Decryption Phase

In order to ensure record safety on cloud, the above hybrid cryptosystem is deployed on cloud. We anticipate cloud server as relied on however so you can prevent tampering/misuse of records with the aid of the usage of intruder or statistics leakage or one-of-a-type safety issues, the records is saved at server with inside the encrypted shape. We extensively classify the scheme deployed on cloud in 3 phases: a) Registration Phase, b) Uploading Phase and c) Downloading Phase.

We used Open Nebula toolkit to line up cloud's environment. In Open Nebula, we've were given had been given one the front node and n cluster nodes. The VM are deployed from the front node to the corresponding cluster node. Open Nebula has been designed in such how that it allows integration with many several hypervisors and environments. There is a the front-surrender that executes all of the approach in Open Nebula at the same time as the cluster nodes offer the reasserts which can be wanted with the aid of the usage of VM. There is at least one bodily community becoming a member of all of the cluster nodes with the frontend.

1. **Registration Phase:** In the Registration Phase, the consumer registers himself so you can add and endure in thoughts his documents to/from the cloud server. In the registration device, the consumer sends its request to the front node and reciprocally, the front node assigns the VM of the cluster node, which has minimal load amongst one-of-a-type VM at the community to the consumer. At the pinnacle of registration phase, the consumer is registered with IP cope with of corresponding VM. Whenever he yet again troubles his request, the request is transferred to its corresponding VM. The encrypted documents, encrypted blowfish keys, public SRNN keys are saved at his registered VM.
2. **Uploading Phase :** In the Uploading Phase, steps are follows:
   Step: 1: The consumer will supply request to the front node to authenticate himself.
   Step 2: On a hit authentication, the front which supply the corresponding IP cope

with of the VM in opposition to which purchaser have come to be registered.

Step 3: The documents are uploaded with the aid of the usage of the consumer to the registered server (VM).

Step 4: The encryption of uploaded documents is finished the use of the hybrid cryptosystem.

Step 5: The encrypted slices and Blowfish encrypted keys stay saved in statistics preserve.

Step 6: The SRNN personal keys are supply to purchaser and in the long run they are deleted shape the server certainly so simplest the authenticated purchaser is able to have a take a have a look at his uploaded record.

3. **Downloading Phase:** In the downloading phase, the stairs are as follows:

Step 1: The consumer will supply request to the front node to authenticate himself.

Step 2: On a hit authentication, the front which supply the corresponding IP cope with of the VM in opposition to which purchaser have come to be registered

Step 3: The consumer will add n SRNN personal keys for the corresponding n slices.

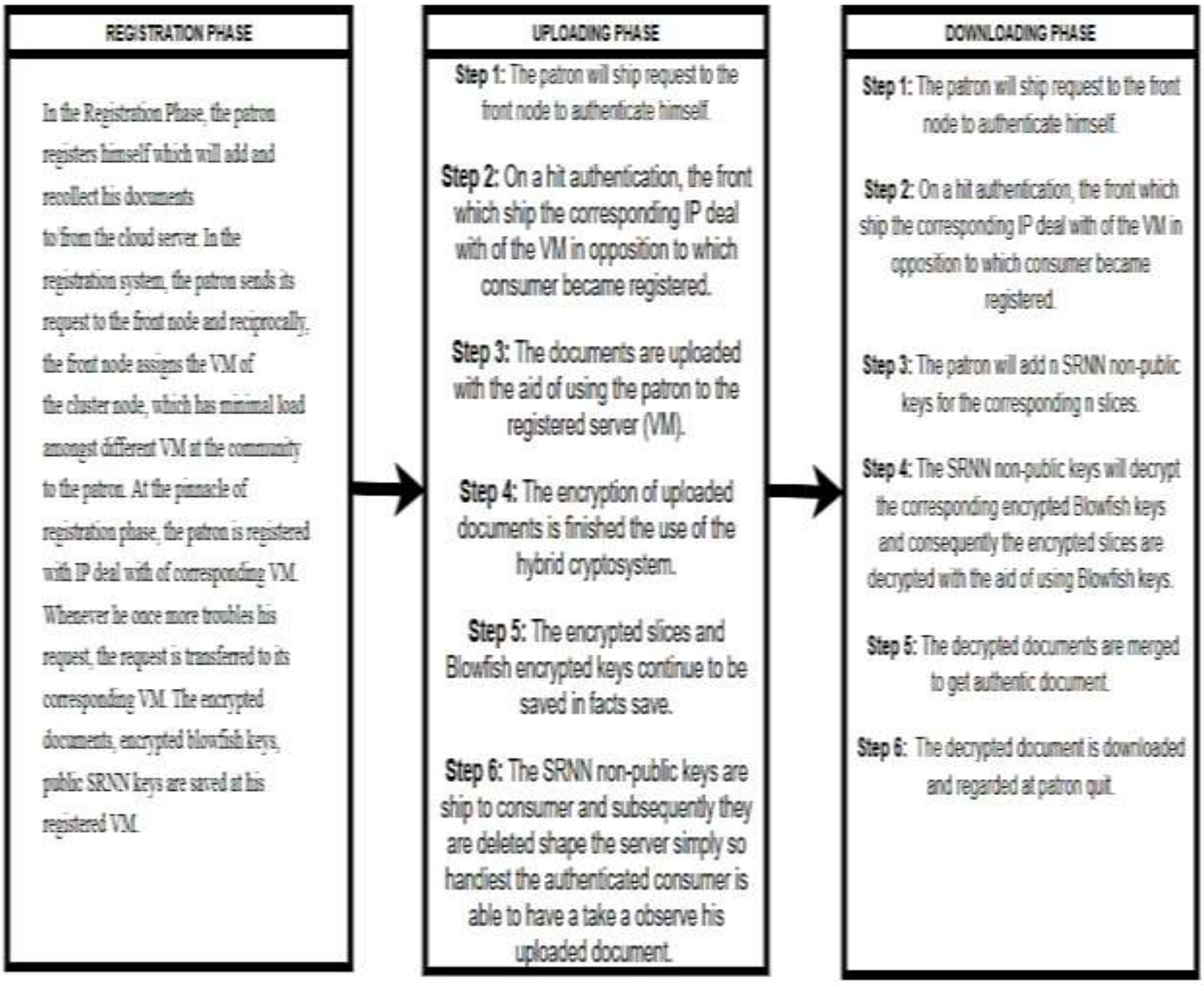
Step 4: The SRNN personal keys will decrypt the corresponding encrypted Blowfish keys and consequently the encrypted slices are decrypted with the aid of the usage of Blowfish keys.

Step 5: The decrypted documents are merged to get genuine record.

Step 6: The decrypted record is downloaded and seemed at consumer surrender.

V. CONCLUSION

The critical intention of this tool is to soundly maintain and retrieve records on the cloud that is exquisite controlled via the owner of the records. Cloud storage issues of records safety are solved the use of cryptography and steganography strategies. Data safety is finished the use of RC6, 3DES and AES algorithm. Key records may be very properly stored the use of LSB method (Steganography). . With the help of the proposed safety mechanism, we have got were given had been given completed better records integrity, immoderate safety, low delay, authentication, and confidentiality. In the future we're capable of add public key cryptography to avoid any attacks in the long run of the transmission of the records from the consumer to the server. The proposed method promises protection and privacy of consumer sensitive records with the aid of the usage of storing statistics at some point of unmarried cloud, with the use of AES, DES and RC2 sets.



REGISTRATION PHASE

In the Registration Phase, the patron registers himself which will add and recollect his documents to/from the cloud server. In the registration system, the patron sends its request to the front node and reciprocally, the front node assigns the VM of the cluster node, which has minimal load amongst different VM at the community to the patron. At the pinnacle of registration phase, the patron is registered with IP deal with of corresponding VM. Whenever he once more troubles his request, the request is transferred to its corresponding VM. The encrypted documents, encrypted blowfish keys, public SRNN keys are saved at his registered VM.

UPLOADING PHASE

Step 1: The patron will ship request to the front node to authenticate himself.

Step 2: On a hit authentication, the front which ship the corresponding IP deal with of the VM in opposition to which consumer became registered.

Step 3: The documents are uploaded with the aid of using the patron to the registered server (VM).

Step 4: The encryption of uploaded documents is finished the use of the hybrid cryptosystem.

Step 5: The encrypted slices and Blowfish encrypted keys continue to be saved in facts save.

Step 6: The SRNN non-public keys are ship to consumer and subsequently they are deleted shape the server simply so handiest the authenticated consumer is able to have a take a observe his uploaded document.

DOWNLOADING PHASE

Step 1: The patron will ship request to the front node to authenticate himself.

Step 2: On a hit authentication, the front which ship the corresponding IP deal with of the VM in opposition to which consumer became registered.

Step 3: The patron will add n SRNN non-public keys for the corresponding n slices.

Step 4: The SRNN non-public keys will decrypt the corresponding encrypted Blowfish keys and consequently the encrypted slices are decrypted with the aid of using Blowfish keys.

Step 5: The decrypted documents are merged to get authentic document.

Step 6: The decrypted document is downloaded and regarded at patron quit.

VI. REFERENCES

1. *Madan S, Techniques for Enhancing Sensitive Data Security in Cloud, IJIACS - UGC (No.- 47464), Vol 6 Number 8 , pp-100-105, Aug 2017*
2. *Madan S., Goswami P., K-DDD measure And map-reduce based anonymity model for secured Privacy preservation big Data publishing, IJUFKS, Vol 27, issue 2, pp 177-199, 2019*
3. *C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy? ," IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, 2018.*
4. *Sinchana MK, Savithramma RM ,Survey on cloud computing security. In: Innovations in computer science and engineering. Springer, vol-224 , pp 1–6 ,2020*
5. *Adviti Chauhan, Jyoti Gupta, A Novel Technique of Cloud Security Based on Hybrid Encryption by Blowfish and MD5, 4 th IEEE International Conference on Signal Processing and control , pp 129-140 January 2018*
6. *Jankowski, K., & Laurent, P., Packed AES-GCM Algorithm Suitable for AES/PCLMULQDQ Instructions. IEEE Transactions on Computers,* Vol.4, No.4,*pp 135–138,2011*
7. *Chun-Ting Huang ,Zhongyuan Qin , C.-C. Jay Kuo , Security of Multimedia in Cloud using Secret Shared Key, International Conference on Computing , Vol 143, Pp 765-775, 2018*
8. *Mustafa Abbas,Suadad S. Mahdi, S. A. Hussien Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography International Conference on Computer Science and Software Engineering (CSASE) , Vol. 2, Issue 1, pp 44-48, 2020*
9. *Ali Kadhim Bermani, Tariq A. K. Murshedi & Zaid A. Abod, A Hybrid Cryptography algorithm for Cloud Computing Security international journal of Core Engineering & Management Posted ,Vol-8, Issue-10,pp 101-109,2017*
10. *Rawal, B. S., & Vivek, S. S. Secure Clouds Storage and Files Sharing. 2017 IEEE International Conference on Smarts Cloud, Vol. 4, Issue 2, pp 34-38,2017*
11. *Sadiq Aliyu Ahmad; Ahmed Baita Garko ,Hybrid Cryptography Algorithms in Cloud Computing: A Review, 15th International Conference on Electronics Computer and Computation ICECCO, vol. 5, no. 1, pp. 31-37,2019*