International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

Development of Secure File Storage on Cloud using Hybrid Cryptography

Sahana Bisalapur[1], Ninad Patil[2], Rahul R.[3], Rushikesh Tarale[4], Sanket Honashetti[5]

Assistant Professor S.G. Balekundri Institute of Technology Belagavi, India[1]

B.E. Student, Dept of CSE, S.G. Balekundri Institute of Technology, Belagavi, India[2-5]

ABSTRACT:In today's world, security and privacy are the most important commodity. Compromising of privacy may lead to destroying the life of an individual. Now a days Cloud Computing is used in many areas like industries, military, colleges, etc,.to store huge amount of data. We can store and retrieve data on the command of one or many users. Storing data on cloud is a risky process like important files belonging to a company which can reveal confidential information which is not supposed to be revealed other than respective authorities. To provide the solution for these issues there are number of ways. There are numerous techniques such as cryptography, steganography etc., We have taken strongest feature of all the techniques and designed a hybrid cryptographic system involving one of the three strongest algorithms known to man. The algorithms used in this system are AES-256, SHA-256, MD5. The use of 256 bit algorithms makes it impossible to crack. We are using random generator to generate a key which adds to the advantage of encrypting the files. For decryption reverse process of encryption is applied using the same key.

KEYWORDS:Encryption, Cloud, Hybrid Cryptography, Security.

I. INTRODUCTION

With the emergence of Cloud Computing, the data storage security in the cloud has been received widespread attention. People on the one hand, hope to be able to use large cloud storage service to alleviate the pressure of the local storage, on the other hand, worry that cloud service providers may provide the confidential information to a third party without authorization, resulting in data information leakage. Data saved in the cloud are required to be encrypted to guarantee acertain security. Cloud computing is generally thought to include the following several levels of service: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service(SaaS). IaaS provides IT infrastructures as a service over the Internet. PaaS provides computing platform as a service to support the cloud applications. SaaS allows users to use cloud application without installing and running software on their own computers. Data owners have limited control over IT infrastructures. This also means that effective data may be revealed and that the deleted data may still be recoverable. However, the file system is responsible for organizing logical orders of data which is stored among the available blocks on the physical medium, and the file system layer which can call for device driver interface allows files to be read, written and created and deleted. These features led people to consider using it to implement secure storage of data filesystem.[1]

II. OBJECTIVES

- To use Cryptographic techniques to translate original data into unreadable form stored on cloud.
- To access the stored data only by authorized person using hybrid cryptographic techniques.
- File searching is an important objective.
- To make the data access faster by categorizing it in different file types such pdf, doc, mp4, png, etc.
- To generate the hash keys for downloading the decrypted data.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

III. LITERATURE SURVEY

[1]Punam V.Maitri & Arun Verma IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2018) December 15,16- 2018-"Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm".

Now a day's cloud computing is used in many areas like industry, military colleges etc to storing huge amount of data. We can retrieve data from cloud on request of user. To store data on cloud we have to face many issues .To provide the solution to these issues there are n number of ways .Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. In this paper we have introduced new security mechanism using symmetric key cryptography algorithm and steganography .In this proposed system AES, blowfish, RC6 and BRA algorithms are used to provide block wise security to data. All algorithm key size is 128 bit.LSB steganography technique is introduced for key information security. Key information contains which part of file is encrypted using by which algorithm and key.File is splitted into eight parts. Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption Keys are inserted into cover image using LSB technique. Stego image is send to valid receiver using email .For file decryption purpose reverse process of encryption is applied.

[2] 2018 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing—"Secure Storage of Data in Cloud Computing".

Cloud storage brings convenient storage of data, at the same time there are also hidden security issues. Data storage security includes legal access to the data stored in the cloud, namely access authorization and authentication security data sharing and the encryption of stored data to ensure data confidentiality, consisting of the accessibility to effective cryptographic data and inaccessibility to the deleted cryptographic data, using tamper-proof technology to ensure the integrity of the data, as well as using tracking technology to ensure data traceability. This paper focuses on the file systems with secure data deletion. We design a file system which supports secure deletion of data. It uses CP-ABE which supports fine-grained access policy to encrypt files.

[3]International Research Journal of Engineering and Technology (IRJET)—"Secure File Storage on Cloud Using Cryptography".

In this paper we aim to securely store information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality, integrity and ensures availability. The rapidly increased use of cloud computing in the many organization and IT industries provides new software with low cost. Cloud computing is beneficial in terms of low cost and accessibility of data. Cloud computing gives lot of benefits with low cost and of data accessibility through Internet. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers may be untrusted. So sharing data in secure manner while preserving data from an untrusted cloud is still a challenging issue. Our approach ensures the security and privacy of client sensitive information by storing data across single cloud, using AES, DES and RC2 algorithm.

[4]AETSD Journal For Advanced Research In Applied Sciences "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm".

This paper focuses on the file systems with secure data deletion. The analysis consists of data access control, data integrity constraints, user traceability and so on. Secure data deletion, that is, when some keys are destroyed, the cipher texts including their copies in the cloud can never be decrypted. At last, we design a file system which supports secure deletion of data. It uses CP-ABE which supports fine-grained access policy to encrypt files. A large amount of data stored in the cloud in order to facilitate users to share, but not all the data can be shared to all, so data owners need to specified authorized users to share data. Traditional access control is based on the plaintext, which cannot be directly applied in the cloud environment. There needs to realize that an authorized person can access the files (except for deleted files) which he has the right and that an unauthorized person cannot access any of the files at any time. In the early studies of the time-based secure deletion, the time property is used in the access control.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

IV. EXISTING SYSTEM

In existing system single algorithm is used for data encode and decode purpose. But use of single algorithm is not accomplish high level security. If we use single symmetric key cryptography algorithm than we have to face security problem because in this type of algorithm applies a single key for data encode and decode. So key transmission problem occur while sharing key into multiuser environment. Public key cryptography algorithms accomplish high security but maximum delay is needed for data encode and decode. To solve above issues we have introduced new security mechanism.

Disadvantages of existing system:

- Block size of blowfish is low i.e., 64 bit.
- It must get the key to the person out of band not through the unsecured transmission channel.
- RC6 is not universally practical.
- Inter multiplications on rotation.

V. PROPOSED SYSTEM

We propose to develop a website which will provide Encryption, Storing and Decryption of files. Encryption is done using three algorithms. First we encrypt the file using AES-256 then we encrypt that file using SHA-256 and finally to make the encryption more stronger we use the third algorithm that is MD5. We then store the encrypted file in the cloud server where the user can access it using the key which is sent to the registered user's email address. We can store all types of files such as Image, pdf, docx, audio, video, excel sheet. Other combination of algorithms may not encrypt all types of files such as audio and video which has continuous bits of data which may result in loss of data after encryption, but the proposed system is robust enough to encrypt all types of files without any loss of data which makes it useful for real time purposes. AES-256 is the most robust security protocol, it uses higher length key size that is 256 bit. It is useful in encrypting audio and video files.

VI. IMPLEMENTATION

There are 3 main phases in the system:

5.1 Registration Phase:

In the Registration Phase, the client registers himself in order to upload and view his files
to/from the cloud server. In the registration process, the client sends its request to front node and in return, front node assigns the VM of the cluster node, which has minimum load among other VM's on the network to the client. At the end of registration phase, the client is registered with IP address of corresponding VM. Whenever he again issues his request, the request is transferred to its corresponding VM. The encrypted files, encrypted keys, public keys are stored at his registered VM.

5.2 Uploading Phase:

In the Uploading Phase, steps are as follows:
Step 1: The client will send request to front node to authenticate himself.
Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which user was registered.
Step 3: The files are uploaded by the client to the registered server (VM).
Step 4: The encryption of uploaded files is done using the hybrid cryptosystem.
Step 5: The encrypted slices and encrypted keys remain stored in VM's data store.
Step 6: The private keys are send to user and finally they are deleted form the server sothat only the authenticated user is able to view his uploaded file.

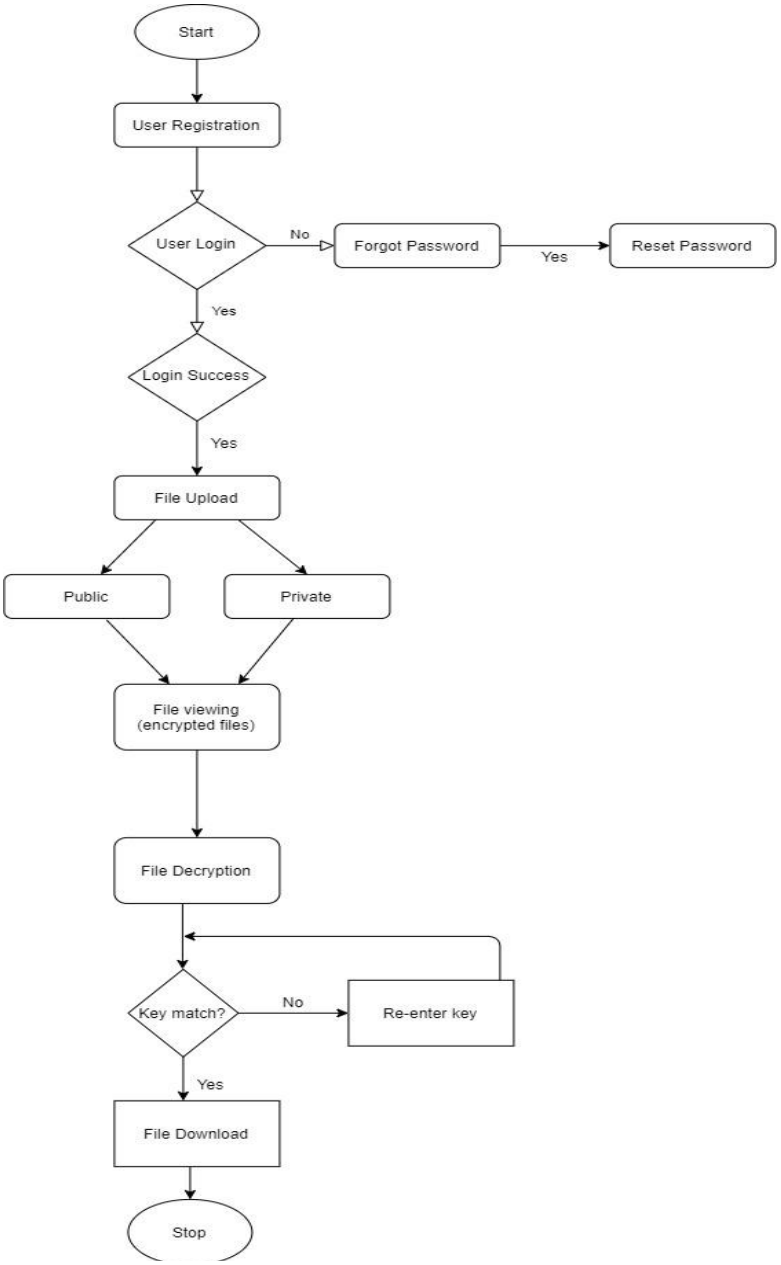
5.3 Downloading Phase:

In the downloading phase, the steps are as follows:
Step 1: The client will send request to front node to authenticate himself.
Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

user was registered.
Step 3: The client will upload n private keys for the corresponding n slices.
Step 4: The private keys will decrypt the corresponding encrypted keys and the encrypted slices are decrypted by keys.
Step 5: The decrypted files are merged to generate original file.
Step 6: The decrypted file is downloaded and viewed at client end.



VII. RESULT

In this proposed system AES, SHA-256, and MD5 algorithms are used for block wise security to data. Proposed system is hybridization of AES, SHA-256, and MD5. The algorithms are combination of symmetric key cryptography and asymmetric key cryptography. These algorithms use a single key for file encode and decode purpose. All algorithms key size is 256 bit. Implementation of proposed system is done using php language. File encoding and decoding time is calculated with the help of php programming. File encode and decode time is calculated for allfiles with comparison of

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

existing AES and Blowfish algorithms. File size is given in MB for AES algorithm. That is 5MB, 8MB, and 10MB. For Encode and decode time calculation of algorithms is done on given file size.

VIII. CONCLUSION

The proposed model is liable to meet the required security needs of data centre of cloud. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. The outcome is securely stored and access data in cloud that is controlled by the owner of the data. We exploit the technique of hybrid cryptography encryption to protect data files in the cloud.

REFERENCES

[1] Punam V.Maitri & Arun Verma IEEE-International Conference On Advances InEngineering, Science And Management (ICAESM -2018) December 15,16- 2018-"Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm".

[2] V.S. Mahalle, A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes)Encryption Algorithm", *IEEE ,INPAC*,pp 146-149,Oct .2014.

[3] 2018 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing—**"**Secure Storage of Data in Cloud Computing".

[4] J. Reardon, D. A. Basin, and S. Capkun. Sok: Secure data deletion. In IEEE Symposium on Security and Privacy, pp. 301-315, 2013.

[5] International Research Journal of Engineering and Technology (IRJET)—"Secure File Storage on Cloud Using Cryptography".