Survey on Secure File Storage on Cloud Using Hybrid Cryptography

Mr. Vaibhav Jaywant Kamble[1] Miss. Afreen Akhtar Nalband[2] Mr.Prateek Nandkishor Sharma[3] Mr. Sohan Subhash Patil[4] Prof. R.S.Barwade[5]

[1,2,3,4,5]Department of Computer Science and Engineering

[1,2,3,4,5]Dr. J. J. Magdum College of Engineering, Jaysingpur, India

Abstract— 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. The proposed model is liable to meet the required security needs of data center of cloud. AES, DES and RSA are used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The idea of splitting and merging adds on to meet the principle of data security. 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. Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.

Keywords: Cloud Storage, Hybrid Cryptography, Security

I. INTRODUCTION

Cloud computing is defined as for enabling suitable, on demand network entrance to a shared pool of configurable calculating resources. Cloud computing everything is delivered as a service, there are three main service models used in the cloud namely: • Platform as a Service • Software as a Service • Infrastructure as a service a) Security issues : Cloud as a method of providing computing resources has many challenges based on design issues which affect the efficiency, security and performance of the entire system, these challenges could be: • Data Storage: Cloud storage providers manage the data in multiple copies across many independent locations • Cloud Confidentiality: Confidentiality can be defined as the sensitive data not being disclosed to unauthorized process, devices and person. A cloud service provider knows where the user's public or private data is located and who can/cannot access the data. • Data Integrity: Data Integrity is defined as the rightness of data stored in the cloud. The alterations between two updates of a record violate the data integrity. • Data Security: In the traditional file systems data was stored within boundaries, but cloud data is stored outside the boundaries of an organization, say, and third party storage using strong encryption techniques. To resolve the above listed challenges, cryptography can provide solutions such as reassuring the receiver/recipient that the message received has not been tampered with or altered – this can be defined as Integrity Checking. This can be achieved by generating a legitimate source and authentication. Securing the database can be a means of securing the cloud. This can be achieved using different encryption/decryption algorithms which are classified as follows:

A. Challenges

Now a days, huge number of organization uses cloud for storing big data and some of the sectors have sensitive data to store for example- Military, Agencies, Collages, Industries, banking etc. The data can be retrieved when the user requests for it. And it is possible for other to access the data. Many issues are faced while storing the data. Solution to these problems is using Hybrid Cryptography. Which will use Encryption and Decryption to 3 number of Algorithms AES, DES, RSA.

II. LITERATURE REVIEW

B. Swathi, And Sri .Dr. Bhaludra Raveendranadh Singh [1] have made cloud storage using cross breed encryption technique. In the proposed model, encryption and unscrambling of records at cloud server is finished utilizing blowfish and altered form of RSA. Atanu Basu, Indranil Sengupta [2] have said that we create a secure cloud storage scheme based on hybrid cryptosystem, which consists of Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and one-way hash function. Here, the data owner exports large volume of encrypted data to a cloud storage provider. The exported encrypted data is over-encrypted by the cloud storage provider, and the data is sent to the requesting user. Swarna C#1, Marrynal S. Eastaff*[3]The paper presents the file security model which uses the concept of hybrid encryption scheme to meet security needs. In the proposed model, encryption and decryption of files at cloud servers done using blowfish and modified version of RSA. Fortine Mata1, Michael Kimwele2, George Okeyo3 [4] we designed a data encryption model that is in charge of storing data in an encrypted format in the cloud. To improve the efficiency of the designed architecture, the service in form of the model designed allows the users to choose the level of security of the data and according to this level different encryption algorithms are used. Kajal Chachapara, Sunny Bhadlawala[5]this paper includes uses cryptography algorithms like AES and RSA. AES is most secure algorithm in cryptography. Once key is generated user (user who have generated a key for their own files) can provide that key to decided user (user for whom key is generated). So when decided user will try to access files on cloud with that key, permission decided by owner will be given to that user.From this we studied that we are also using three techniques to split data into three parts and and send keys which is generated by splitting to the user from owner, if he is a authorized user. So We can securely store data in cloud. Paper which have read uses different techniques, but

here we are going to use some of the techniques from this paper for encryption and decryption.

III. METHODOLOGY

A. Problem Experiment Work

In above papers mentioned, we are going to learn about various algorithms which is used for encryption. Here, we will use the same methods for our model.This paper gives a comparative view of different encryption algorithms on parameters like CPU usage, encryption time, ROM utilization, throughput with different file sizes, length of packet and data type.

1) Rivest - Shamir- Adleman (RSA)

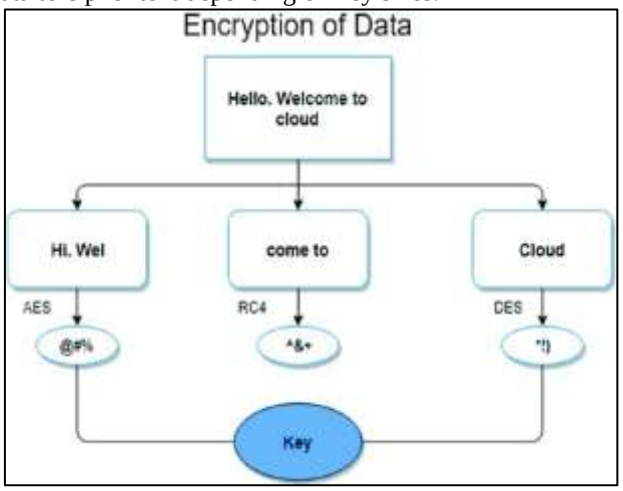
It is a public cryptosystem technique that incorporates block size encryption and variable key size. The steps involved are i Generate two distinct prime numbers. ii. Calculate t as product of two. iii. Now compute phi(t). iv. Find d such that d*e = 1 v. Public Key is (1, e) and Private key is (1, d). Its most apparent disadvantage is if two numbers are of massive length then it takes more time and, they should be of comparable size.

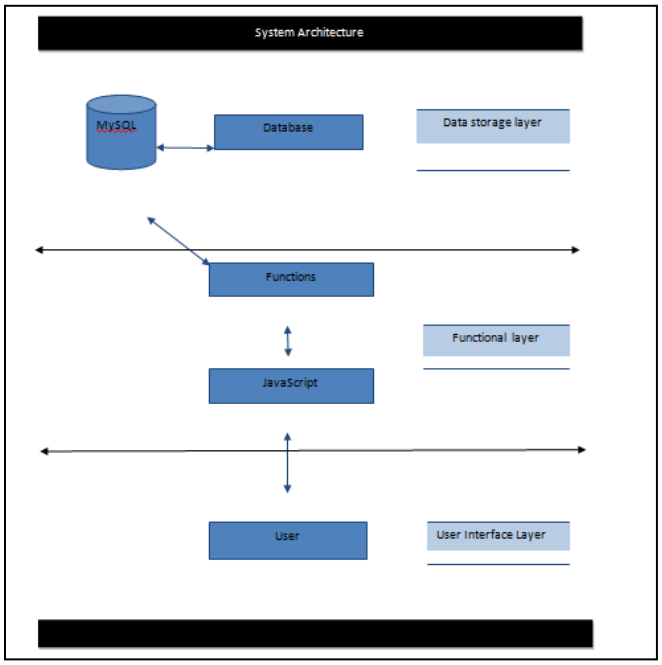
2) Data Encryption Standard (DES)

This encrypt algorithm is the most widely used because it works on bits. It is a block cipher incorporating fiestel structure. Length of message at one time to be encrypted is 64 bits and the key size of 64-bits but every 7x bit is a check bit which is removed in making of sub-keys. The steps involved arei. Cut the plain text in two parts left and right. ii. Design 16 sub keys 48 bits long each. iii. Code words are written for each 64-bit block of data. As known, it is one of the best algorithms because no such possible attack is known to crack it other than brute-force which is costly and time consuming.

3) Advanced Encryption Standard (AES)

AES also known as Rijndael structure is an iterative algorithm rather being called a fiestel structure. It also a block cipher has block capacity of 128 bits and key size any of 128, 192 or 256 bits. It is iterative because it uses rounds to convert data to cipher text depending on key sizes.





IV. HYBRID CRYPTOGRAPHY PHASES

The hybrid cryptosystem used to maintain security of the files has two phases:

– Encryption Phase
– Decryption Phase

A. Encryption Phase

At the encryption end, on the specification of user, the file being encrypted will be split into 3 parts. Each of the file is encrypted using different different algorithms which is mentioned above and key provided by the owner for each part.

B. Decryption Phase

At the decryption end, the user will get 3 private keys, according to the number of parts created during the encryption phase. Key is decrypted at the server, using the corresponding decrypted keys, file slices stored at server are decrypted. The decrypted slices will be merged to generate original file.

V. PROPOSED CLOUD COMPUTING SECURITY ARCHITECTURE

In order to ensure file security on cloud, the above hybrid cryptography is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form. We broadly classify the scheme deployed on cloud in three phases:

– Registration Phase
– Uploading Phase
– Downloading Phase

We used tomcat server to set up cloud environment. Here we

A. Registration Phase

In the Registration Phase, the owner and user registers himself in order to upload and view his files to/from the cloud server. In the registration process, the user sends its request to front node and in return, the Owner check, is it athorable

user, if yes then he send the key to registered email of using front end.

B. Uploading Phase

In the Uploading Phase, steps are as follows:
Step: 1: The client or user will send request to front node to authenticate himself.
Step 2: On successful authentication, the front end or owner which send key to registered email address
Step 3: The files are uploaded by the owner to the registered server or cloud.
Step 4: The encryption of uploaded files is done using the hybrid cryptosystem.
Step 5: The private keys are send to user and finally so that only the authenticated user is able to view his uploaded file.

C. Downloading Phase

In the downloading phase, the steps are as follows:
Step 1: The client or user 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 owner will upload or send private keys for the corresponding email address .
Step 4: The private keys will decrypt the corresponding encrypted keys are decrypted keys.
Step 5: The decrypted files are merged to generate original file.
Step 6: The decrypted file is downloaded and viewed at client end

VI. Results

The stored image file is completely secured as the file is being encrypted not by just using one but three encryption algorithm which is AES, DES, RSA. Data is kept secured on cloud server which avoids unauthorized access. Requires an active internet connection to connect with cloud server. Data security is a major priority. This system can be implemented into banking and corporate sectors to securely transfer confidential data. It is not possible to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:-As the technology emerges, it is possible to upgrade the system and can be adaptable to desired environment. Based on the future security issues, security can be improved using emerging technologies like single sign-on.

VII. Conclusion

The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. We exploit the technique hybrid cryptography encryption to protect data files in the cloud. Two part of the cloud server improved the performance during storage and accessing of data. The hybrid Encryption algorithm used for encryption is another advantage to improve the performance during encryption and decryption process. We assume that this way of storing and accessing data is much secure and have high performance. Our efforts are going on to solve the problem of group sharing of data in the shared data section as in this scheme only member of group can access the data stored over shared data section. One to many, many to one, many to many communication is not possible.

References

[1] B.Swathi, 2 Sri .Dr. Bhaludra Raveendranadh Singh*,"Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm,"*Volume no.06, Issue No.11,November 2017.
[2] Atanu Basu, Indranil Sengupta*," Secure Cloud Storage Scheme Based On Hybrid Cryptosystem".*
[3] Swarna C#1, Marrynal S. Eastaff*2, *"Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm,"* VOLUME 5, ISSUE 3, MAR/2018.
[4] Fortine Mata, Michael Kimwele2, George Okeyo3*," Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish),"*Volume no.6,Issue no.3,March 2017.
[5] Jitendra Singh Adam et al.*," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm"*, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2,Aug. 2012.
[6] Manikandan.G et al., *"A changed cryptographic plan improving information"*, Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.
[7] Niles Maintain and Subhead Bhingarkar, *"The examination and Judgment of Nimbus*, Open Nebula and Eucalyptus", International Journal of Computational Biology, vol. 3, issue 1, pp 44-47, 2012.
[8] Srinivasarao D et al., *"Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm"*, Journal of Global Research in Computer Science, vol. 7, Jul. 2011.
[9] Achill Buhl, *"Rising Security Challenges in Cloud Computing"*, in Proc. of World Congress on Information and correspondence Technologies ,pp. 217-222, Dec. 2011.
[10] Tingyuan Nye and Tang Zhang "*An investigation of DES and Blowfish encryption algorithm"*, in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.
[11] Peter Mel and Tim Grace, *"The NIST Definition of Cloud Computing", NIST, 2010.*

