Data Security Using Client Side RSA Encryption Method in Cloud

Dhara Patel[1], Prof. Rajyalakshmi Jaiswal[2]
[1] *Pursuing ME in Wireless and Mobile Computing of Computer Engineering, GTU PG School, Gandhinagar, Gujarat, India.*
[2] *Assistant Professor at L.D. College of Engineering, Ahmedabad, Gujarat, India.*

ABSTRACT

nowadays every platform have cloud storage like Google, Apple, Amazon and Any other data Most of them are store the data to the cloud. So the storing data on third party's system causes serious concern on data confidentiality. To improve and provide the cloud security we are using the various cryptography algorithms. Secure data forwarding in cloud using the RSA algorithm is the one way to securely forward your data. Using RSA user encrypt the file and store to cloud using the public key and other who wants to access the file they enter the private key and decrypt it. This is the traditional technique for data forwarding, but for the more security they introduce re-encryption concept. In which your will be encrypted twice.

Keyword: - *Cloud Storage, Secure Data,Data Confidentiality ,RSA algorithm,Re-Encryption.*

1. INTRODUCTION

A cloud is the platform for storing the data. It is the place where we can share the any types of the data like documents, databases, media, personal data, etc...But, we must have to provide security for the data. There are multiple ways to provide the security. And we have to choose best of them. Cryptography is the one of the effective way to provide the security to any type of data.

There are two types of cryptography algorithms Symmetric key algorithms and Asymmetric algorithms which are very useful to provide tight security.. The symmetric algorithm contains AES, DES, and Blowfish. The Symmetric algorithm is fast and suitable for large amount of data but problem with the symmetric algorithm is key sharing. The key sharing process is the most effective because there is the fear of key theft and losing the data. So we have to be very careful at a time of key sharing

.In asymmetric algorithm we have two types of key one is Public key and other is the Private Key. The public key is use to encrypt data and the private key is use to decrypt data. Both public key and private keys are mathematically related to each other. Only associated private key can decrypt data. Both keys are unique. Asymmetric algorithms are like Diffie Hellman, DSA, El-Gamal, RSA, etc… These Algorithms are used to provide high level security and do not require any initial key exchange between sender and receiver. These types of algorithms are used to open network. In Real time of applications both types of algorithms are used to provide tight better security.

1.2 Objective

The lack of strong security control of user´s private information that led theft the information from stored in the device. Save information is not in secure encrypted media. The Data robustness is a major requirement for storage systems. The re-encryption scheme secures the data. The RSA is best encryption algorithm for securing the data. The results show that RSA is secure algorithm for the Encrypt the data.

2. CLOUD STORAGE OVERVIEW AND BACKGROUND

Here the overview of the cloud storage and background of it.

A. Cloud Storage Overview and Background

Cloud is platform of on demand network access of computer resources like networks, servers, applications, services, and storage. Cloud is increase the running capacity of device because of minimal load on the device and after once upload on cloud it is accessible anywhere. Cloud is allowing using applications on internet, and that store and protecting your data while providing the services, for example e-mailing. It also provide the storage for business, personal data, etc…

Cloud is on-demand deployment, internet services, and open source platform. Cloud is using the virtual servers to store the data. The virtualization allows them to fast and easily update the users activities.

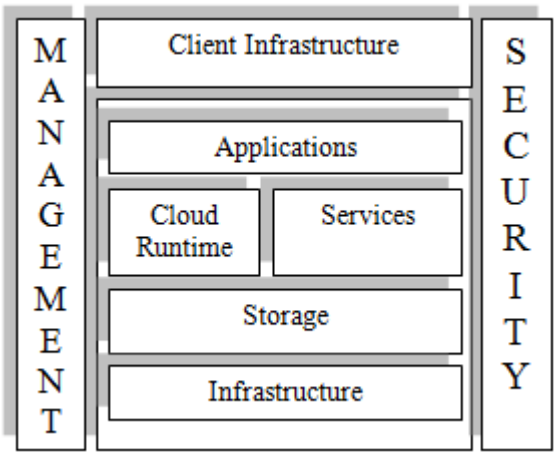

Fig 1: Cloud Computing Architecture

There are three types of infrastructure models Public, Private, and Hybrid cloud. Public cloud runs by third parties like Google, and applications are used by the different customers. Private Cloud is built for the private use of one person, providing the most control over data, security, and requirement of users. Private cloud are built by own companies. Hybrid Cloud is combination of private and public cloud.

B. Architecture Layers of Cloud

There are three Layers in cloud first is Software as a service, second is Platform as a Service and third is Infrastructure as a Service.

Software as a Service (Saas): Saas is the feature a complete application service on demand. One instance run cloud and services multiple end users as client companies.

Platform as a Service (Paas): Paas provide service that is used to build high level service. There are two possibilities in Paas one of that produce Paas and other one is using the service. Paas provides every phase of software development process, like maintaining, testing, developing, etc…

Infrastructure as a service (Iaas) : Iaas is the basic storage standardized services over the network. It offers more storage space to users.

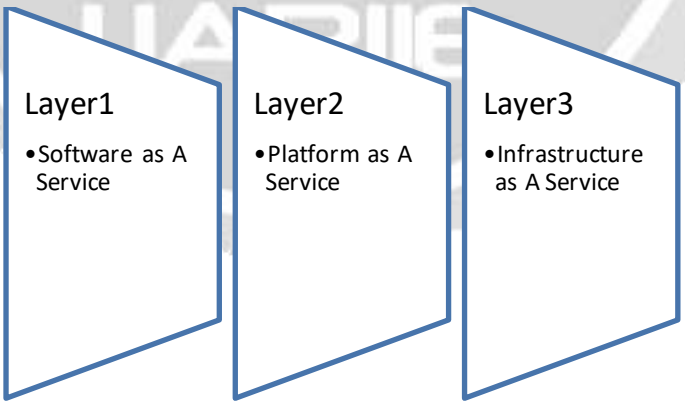

Fig 2:Architecture Layers of Cloud

C. Issues in Cloud

Here are several issues of cloud platform:

- **Cost** There are different-different cost of the public cloud and private cloud.

- **Speed** The cloud gives you more flexibility to control the speed of your device. But sometimes it takes much time to upload or retrieve data.

- **Security** The cross Cloud communication is performed over the public Internet so there is fear of data theft and hacking of the personal information. If any business data then any attack can destroy the data so we have to overcome these issue.

D. Solution over Issues on Cloud

Different Encryption techniques are there for these issues in cloud. The encryption of the data is the secure way to the protect data. But sometimes it is not efficient. There is re-encryption method for more security till now method is only at server side, so there is possible way that we can implement it on client side. For the more security we can track data and do the time analysis for the any type of data. For speed we go through time analysis we can track the speed and time for the same size of the file. The time analysis of the uploading and downloading will be track by the time analysis function. We can combine the cryptography with the time analysis function so our two motives will be solving in the one implementation. We can use the cryptography for provide the security, data robustness and data confidentiality.

3. Secure Data Forwarding

In the Cloud we are sharing the data among each other but from where we are share the data and from where we are retriving. Also do not know that it is secure or not for that reason we rrequire data security at the time of forwardd the data. There differenr secure ways to protect data.one of the most effiecient way is cryptography. So we have to encrypt the data.There are following steps to forward the data.

Uploading Data which is to be updated from the anuser which is encrypted and then save to the server, and other user who wants retrieve the data then have to decrypt it with key and then he/she can use it.

Forwarding Data Forwarding is the process of forward the data from one user to other user using cloud.So the sender encrypt with the public key and receiver decrypt with private key and get the data.

Retrieving Data retrieval has two retrievals one for the sender and one for the receiver. If sender wants to get the data then the encrypted data is retrieved from the data servers before it is decoded and then sent to the sender there each decoded encrypted parts are decrypted by using the secret key of the sender which is requested from the key servers and then combined for the complete data.

Deleting Data deleting could be done using key entering, If user wants to delete data from the source then he/she have enter the key. Anyone can not directly perform delete performance. The user can use the same key as encryption to delete the data from the server.

3. RE-ENCRYPTION

The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. As mention above the re-encryption is the process of encrypts data twice. Previous encryption algorithm provides the limited protection and because of that there is fear of data theft, data lost at the time of upload or download. Due to this it's easy to access the data from server. So we need more security for the data. The re-encryption of the algorithm is done two ways. First is the re-encrypt the key and second is re-encrypt the data. The Re-Encryption of the data is done at time of uploading on server. And will do at time of download and again through previous algorithm. The Re-encryption improves the security when the data is stored on the cloud. Without secret key nobody can access the data. There is twice encryption on the data. So if anyone wants to crack the data it is not easy. The client side re-encryption is the done with two process the first one is the normal encryption the second one encrypt the file when user wants to upload on the server. So the data is encrypting twice. So the decryption process is same as the encryption. Users have to decrypt the data twice. First one is at time of download and second one is normal decryption. At last the user will get the normal data.

RSA Algorithm:

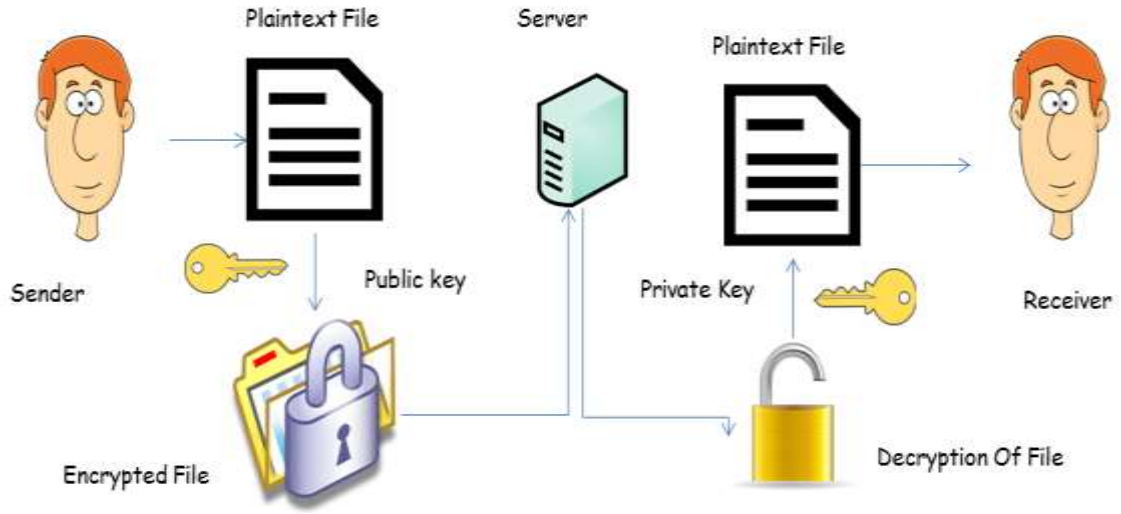

Fig 4.1.1.1 Basic RSA Algorithm

Key Generation
A Key Generation: KeyGen(p, q)

Input:

1. Take two large primes – p, q
2. Compute n = p *q
3. Compute φ (n) = (p - 1)*(q – 1)
4. Select the public exponent $e \varepsilon \{1, 2 \ldots, \varphi(n)-1\}$ such that gcd$(e, \varphi(n)) = 1$
5. Compute the private key d such that $d * e \equiv 1 \bmod \varphi(n)$

Key: Public key = (e, n), Private Key= (d, n)

A. Encryption

$C = M^e \bmod n$ // where C is the Encoded text and M is the Decoded text.

B. Decryption

$M = C^d \bmod n$ //where C is the Encoded text and M is the Decoded text.

Cloud Server Amazon S3 Connection The cloud server connection with server is done also with java. All the data of web application will be store on could server.

1. Create the console account in aws.amazon.com
2. Select the type of Users and accept the policies of amazon web services.
3. Install the AWS SDK to IDE and accept polices.
4. Create the security credentials and get the "access key" and "access id".
5. In S3 create new Bucket and in bucket create Object. This is the process to connect the amazon web services. After that we can use the services and storage of the amazon web server. We can store data in bucket and perform operation any operation on it even we can provide server side encryption also.

4. RESULTS & ANALYSIS:

1. Encryption & Re-Encryption Time

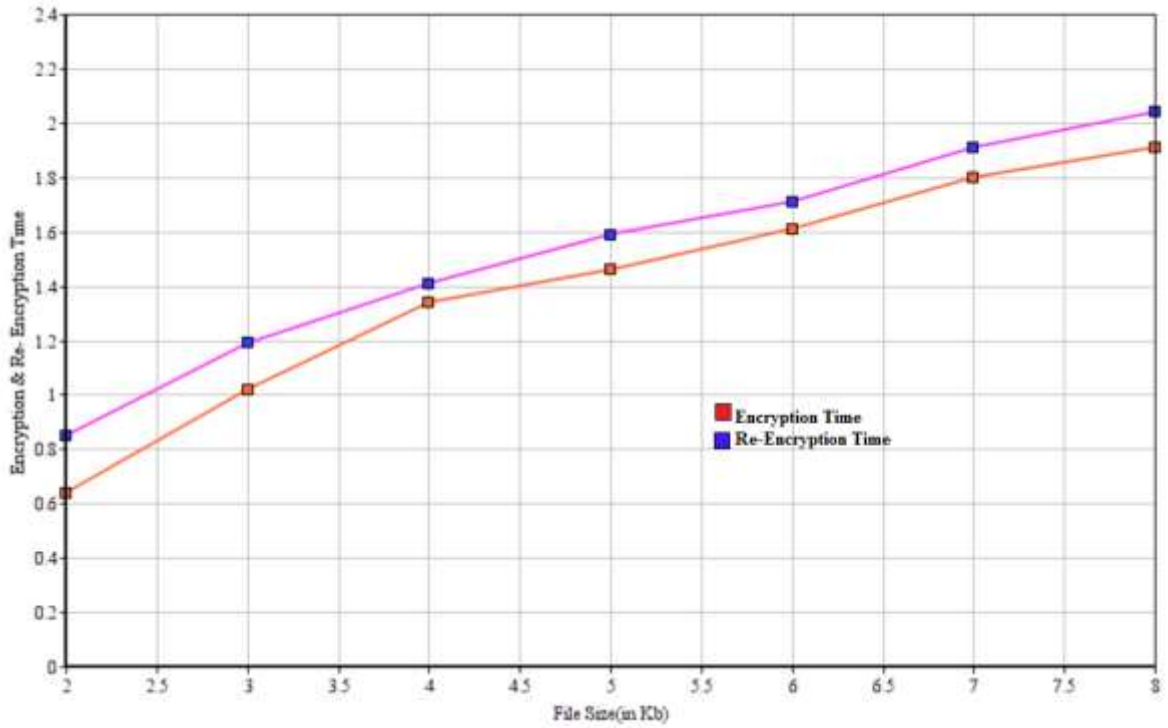

Fig: 4 Encryption Time for RSA Algorithm

2. Decryption & Re-Decryption TIME

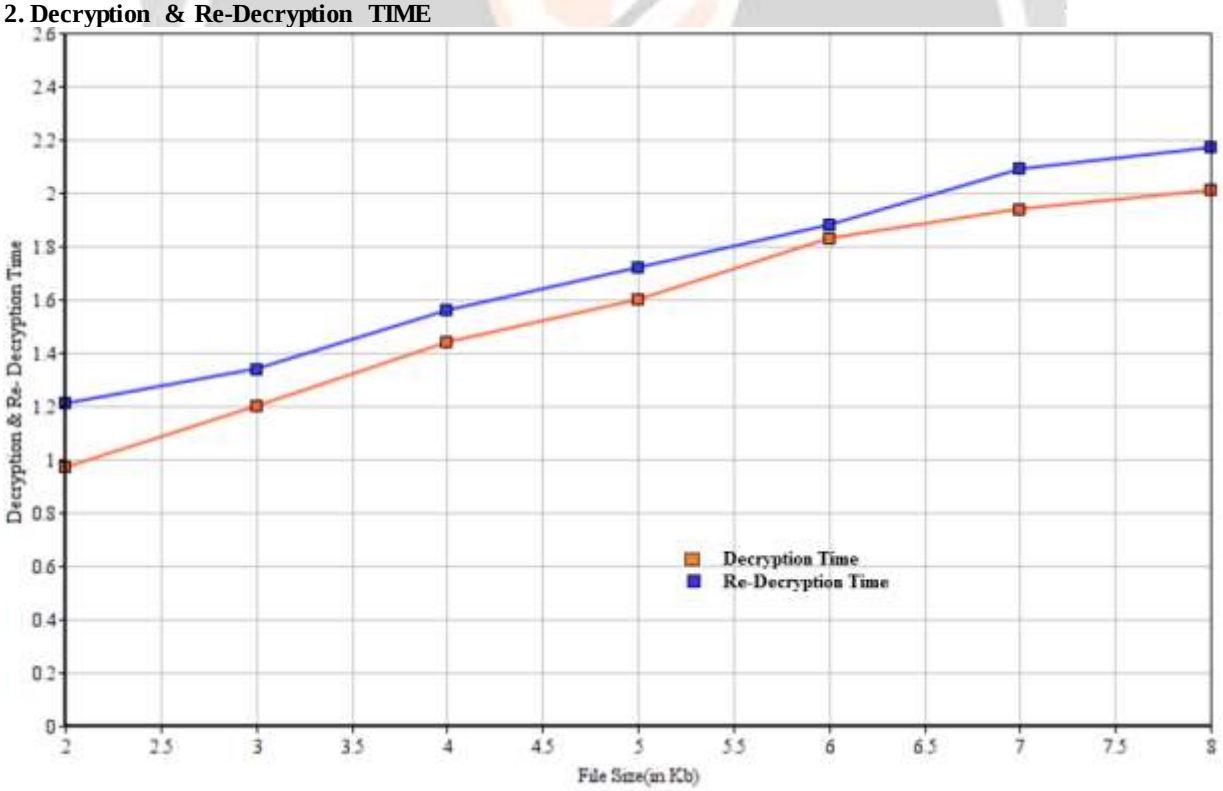

Fig: 5 Decryption Time for RSA Algorithm

5. CONCLUSION

The data forwarding from one user to another user by traditional encryption way cause the data confidentiality problem it's better to consider the re-encryption scheme to forward and retrieve data because this is very secure way to communication. It will be propose a new re-encryption scheme and integrate it with a mobile platform using RSA

algorithm because till now it's most secure asymmetric algorithm which is widely used over internet for security purpose. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages.

6. REFERENCES

[1] Prabha, K.; Nalini, S. "A secure data forwarding in cloud storage", Optical Imaging Sensor and Security (ICOSS), 2013 International Conference on, On page(s): 1 – 4

[2] Seung-Hyun Seo.; Mohamed Nabeel,; Xiaoyu Ding.; Elisa Bertino."An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds", IEEE Trans. On Knowledge And Data Engineering, VOL. 26, NO. 9, SEPTEMBER 2014.

[3] Renjith, P.; Sabitha, S. "Verifiable El-gamal re-encryption with authenticity in cloud", Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on, On page(s): 1-5

[4] M. Al-Hasan, K. Deb, and M. O. Rahman, "User-authentication approach for data security between smartphone and cloud", 8th Intel Forum on Strategic Technology (IFOST '13) IEEE, vol. 2, on page(s): 2-6, 2013.

[5] Nasrin; Zurina Mohd Hanapi; A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014

[6] Mazhar Ali,Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V.Vasilakos, Keqin Li, Albert Y. Zomaya, Fellow, " SeDaSC: Secure Data Sharing in Clouds ", Computers, IEEE Transactions on, On page(s): 941 - 953 Volume: 63, Issue: 4, April 2014.

[7] Sowmya Sri, *S.Vikramphaneendra*, "A Secure Way for Data Storage and Forwarding in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering. , Issue: 10, January 2015

[8] Mohammad Ahmadi, Faraz Fatemi Moghaddam,Amid Jamshidi Jam, Somayyeh Gholizadeh, Mohammad Eslami," A 3-Level Re-Encryption Model to Ensure Data Protection in Cloud Computing Environments ",2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 ,2014

[9] Kajal C.,Sunny B.,"Secure Sharing with Cryptography in Cloud Computing" 2013 IEEE, Nirma University International Conference on Engineering(NUiCONE),On Page(s): 1-4.

[10] Faraz F. Moghaddam, Iman G., shirin D. Varnosfaderani, Soroush Mobedi, " A Client Based User Authentication and Encryption Algorithm for Secure Accessing to Cloud Servers." 2013 IEEE Student Conference On Research and Development(SCOReD), 16-17 December 2013 ,Malaysiya,On Page(s):175-180.

[11] Randeep K., Supriya K., "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014.

[12] Sura Khalil Abd., Azizol A., "A Review of Cloud Security Based on Cryptographic Mechanisms." IEEE 2014 International Symposium on Biometrics and Security Technologies (ISBAST),On Page(s):106-110.

[13] Akanksha U., Monika B.,"Deployment of Secure Sharing : Authenticity and Authorization using Cryptography in Cloud Environment" IEEE *2015* International Conference on Advances in Computer Engineering and Applications (ICACEA)Ghaziabad. On Page(s):852-855.

[14] Preeti G., Vineet S., "An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function" IEEE 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) On Page(s): 334-339.