Secure Data Forwarding in Cloud Using AES Algorithm

*Riddhi Ghevariya, **Rajyalakshmi Jaiswal

*GTU PG School at Ghandhinagar

**L.D. College of Engineering

ABSTRACT

In today's world, leading IT giants are encouraging and approaching toward cloud storage like Google, Microsoft, Apple, Amazon and other similar companies are offering data storage in cloud for end users. We know that storing the data on third party's system causes serious concern on data confidentiality. To enhance and provide the cloud security, various cryptography algorithms are used. Secure data forwarding in cloud using AES(Advanced Encryption Standard) algorithm is one of the safest way to securely forward the data. AES encryption and decryption is highly secured and fastest technique. Client side encryption is an effective approach to provide security to data before forwarding it on a cloud storage. This is the traditional technique for data forwarding, now to take security to next level, re-encryption concept is introduced, in which data will be encrypted twice.

Keywords—*Cloud Storage; Secure Data;Data Confidentiality ;AES algorithm; Re-Encryption.*

I. INTRODUCTION

Cloud is remote virtual place where we can store and share any type of data like documents, databases, media, personal file, etc...Though, we ought to provide essential security for the data. There are multiple ways to provide the security and we shall choose best among them. Cryptography is the one of the effective way to provide the security to any type of data. The cryptography algorithms are categorized into two types, which are very useful to provide robust security. Symmetric key algorithms and Asymmetric algorithms.

In asymmetric algorithm we have two types of key one is Public key and other is the Private Key. The public key is used to encrypt data and the private key is use to decrypt data. Both public key and private keys are 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.

The symmetric algorithm contains AES, DES, and Blowfish. In symmetric key cryptography every user have own secret key. Only one secret key is used for encryption as well as decryption.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 loosing the data. So we have to be very careful at a time of key sharing. AES is a block cipher algorithm which has 3 fixed 128-bit block with three keys i.e. 128-bits,192-bits 1nd 256-bits. The maximum block size is 256-bits. And It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. In Real time applications, both types of algorithms are used to provide as per the security requirements.

Objective

The lack of strong security control of user´s private information that leads to malicious attack, which compromises the information from stored in the device. The Data security and robustness is a major requirement for storage systems and to do so, we are going to introduce re-encryption method. The AES is best encryption algorithm for securing the data and we will use the same for re-encryption.

II. CLOUD STORAGE OVERVIEW AND BACKGROUND

Here is the overview of the cloud storage and background associated.

1.Cloud Storage Overview and Background

Cloud computing is divided into two parts: The first part is known as front-end and the other one is back-end. Both are connected to each other via Internet. The front-end includes the client system. System application is required to retrieve the cloud computing data. The back-end part consists several computer systems, server nodes and data storage systems that develops the cloud of the computing service. The central server's task is to administrate the system, monitor the trace and meet client demands to ensure that everything runs smoothly. It follows a different set of rules known as protocol and uses a special type of software which is called as middleware. The Middleware facilitates communication between the network computers to collaborate with one another.

Cloud computing is a rapidly growing computing model all over the world. In cloud computing, resources of the computing communications are provided as services over the Internet. Storing data into the cloud offers great help to users since they do not need to worry about the complexities of hardware management.

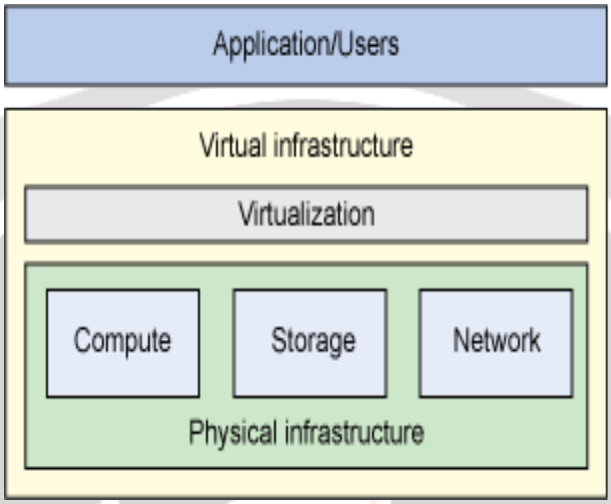


Fig 1: Cloud Computing Architecture

There are three types of cloud deployment models as Public, Private, and Hybrid cloud. Public cloud runs by third parties, it is available to end users and large industries. This type of cloud is developed for selling cloud services. Private Cloud is a cloud which is build for a particular organization. It provides the most control over the data security. Hybrid Cloud is combination of above two.

2. Architecture Layers of Cloud

The cloud architecture is divided into three layers. The first is Software as a service, second is Platform as a Service and the last is Infrastructure as a Service.

Software as a Service (Saas): It is a distributed model in which application are installed by the vendor or cloud provider and it is made available for end users over Internet.

Platform as a Service (Paas): It is a platform environment that allows developers to develop, run and manage Web applications without the complexity of building and maintaining the infrastructure e.g. Google play store.

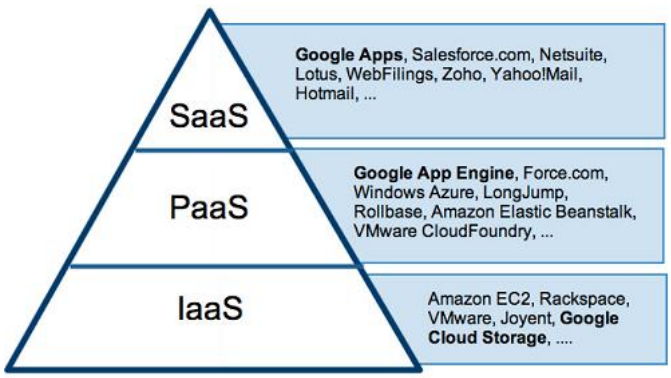


Fig 2:Architecture Layers of Cloud

Infrastructure as a service (Iaas) : IaaS provides the underlying operating systems, networking, security, and servers for developing such applications, services, and for deploying development tools, databases, etc.

3. Issues in Cloud

Here are the major concerns of cloud platform:

- **Cost:** The cost of cloud is higher than the traditional storage system.
- **Speed:** The cloud provides more flexibility to control the speed of your device though sometimes it takes much time to upload or retrieve data (due to variation in speed).
- **Security:** The cross Cloud communication is performed over the public Internet so there is a fear of data theft and hacking of the personal information. Any vulnerable attack can destroy the data, so these issues must be overcome.

4. Solution over Issues on Cloud

There are different techniques used to resolve these issues. Secure way to protect the data is encryption method. However, sometimes that is not good enough. We need thrive for more security. So re-encryption method is being used to get maximum level of security, Currently it is being used at only server side, so implementing it on client side has a bright future. In order to get more security, tracking the date and time analysis of any date can be useful. To overcome the issue of speed, we take a look at time analysis, speed and time for the same size of the file can be tracked. Time analysis function will track the uploading and downloading. So our two objectives can be compiled into one motive by combining cryptography with the time analysis function. Cryptography is used to provide security, data robustness and data confidentiality.

III. SECUREE DATA FORWARDING

Different types of data are being shared over the network from one end to another. We are not concerned about the security of the data while sending or retrieving it from the cloud. While retrieving the data we are not sure about the security of the data that if it is being compromised or not. For the reason being, it is required to make sure that at the time of data forwarding, it is secured. Most efficient way to protect the data is cryptography. Following are the steps to forward the data.

Forwarding: Data Forwarding is the process of transmitting the data from one user to the other using cloud. The data is encrypted with the key and to decrypt it, one has to use the same key which was used at the time of encryption of the data.

Retrieving : Retrieval can be done in two ways. One for the sender and the other is 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

Updating: After updating the data, user has to encrypt before saving it on the server. If any other user wants retrieve the data, then he/she has to decrypt it with the same encrypted key. The each part or block of the data is encrypted or decrypted using the same key. If you do not enter the key at a time of updating the data, then the alteration can't be saved.

Deleting: If a user wants to perform deletion operation on a data in cloud, then he/she has to enter the encryption key. One can not delete any data from a cloud without the encryption key.

IV. RE-ENCRYPTION

The encryption technique improves the security of data. We can use different type of algorithm to encrypt the data or encode a message. After doing so we can safely forward it over a network. The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding. The process of Re-Encryption increases the security while storing the data in the cloud environment. These high level security mechanisms reduce the security breach while storing the files in the cloud environment. This security mechanism provides the secure transaction of files between users and the Cloud Environment. The AES encryption algorithm is widely used for the data communication and it is most secure algorithm that exists. Normal AES encryption has variable key length of 128, 192, or 256 bits; default 256, while the round operations are 10, 12 and 14 respectively. We can use any length of key to perform re-encryption which is nothing but the encryption of encrypted data. We can also use RSA algorithm for the re-encryption as well.

AES Algorithm:

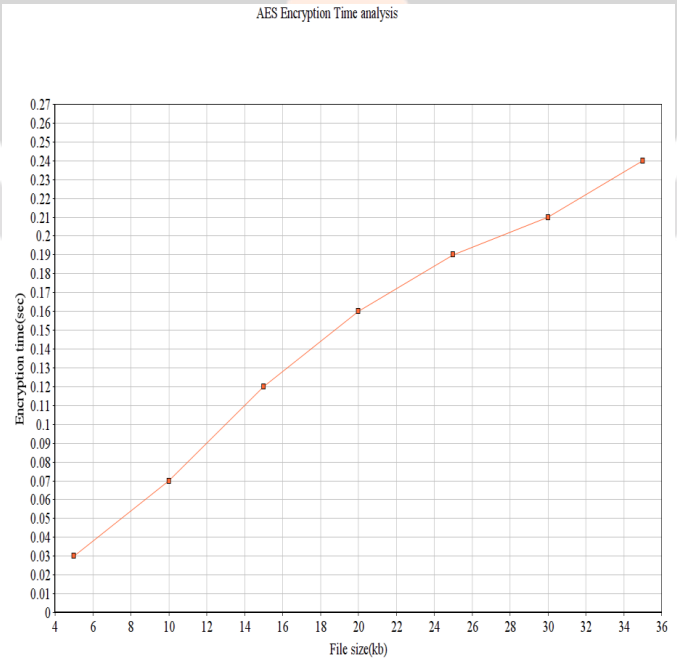
1. **Key expansion –** from rijandael's key schedules derives round key from its ciphers.
2. **Intial round –**
   a. Add round key – by using bitwise XOR combine each bit with round key.
3. **Rounds –**
   a. Sub bytes – each byte is replaced with another using a look up table as a non linear substitution.
   b. Shift rows – each row is shifted cyclically to a number of times called transposition.
   c. Mix columns – combines four bytes in each column.
   d. Add round key
4. **Final round –**
   a. Sub bytes
   b. Shift rows
   c. Add round key

V. CLOUD SERVER AMAZON S3 CONNECTION

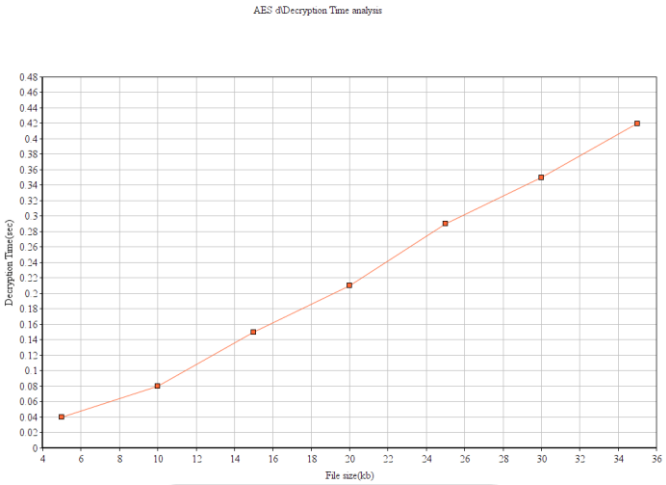
We will use the eclipse mars along with java language to develop a web application through which we will get the access to the our Amazon console account and data will be stored on cloud server.
Following are the steps:
1. Create the console account in aws.amazon.com
2. Select the type of Users and accept the policies of Amazon web Services.
3. Install the AWS SDK to IDE and accept polices.
4.Generate the security credentials to get the "access key" and "access id". Generate the security credentials to get the "AWSAccessKeyId" and "AWSSecreteKey"
5. We will create bucket in S3 followed by object creation in the bucket. 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 and we can also provide server side encryption.

VI. Performance Analysis of AES

Now we will see the encryption time analysis as well as decryption time analysis by uploading a file. Here file size will be in kb and the time will be in second.



From the above graph, we can say that the algorithm is taking 0.24 second to encrypt a file size of 35 kb.



From the above graph, we can say that the algorithm is taking 0.42 second to decrypt a file size of 35 kb. So we can say that the decryption time is almost double then the encryption time.

Conclusion And Future work

We have presented an approach by which we can provide more security to our file or data so that we can achieve confidentiality. With this method, client can provide better security to data which is not present in existing public cloud system. To achieve the data confidentiality, we have suggested client side re- encryption and re-decryption technique using single secret key. We can store our file on a public cloud (Amazon S3) in encrypted format and after that we can also encrypt the encrypted data using AES algorithm. So that way we explored AES re-encryption and re- decryption scheme to make cloud users data secured and also guarantee the data privacy in the cloud.

The future research should address the development of a framework through which the data or any type of file will be re-encrypt before storing it on a public cloud. So the trust on "third party" issue can be resolved at most.

REFERENCES

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

[2] Niteen Surv, Balu Wanve, Rahul Kamble, Sachin Patil, Jayshree Katti; "A Framework for Client Side AES Encryption Technique in Cloud Comput- ing", IEEE International Advance Computing Conference (IACC)2015,On Page(s):526-528,2015.

[3] Manpreet K.,Rajbir S.; "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications (0975 – 8887)Volume 70– No.18,On page(s):16-21, May 2013.

[4] Akhil Bhel,Kanika Behl; "An Analysis of Cloud Computing Security Issues", 2012 IEEE World Congress on Information and Communication Technologies, On Page(s):109- 114,2012.

[5] Randeep K.,Supriya K.; "Analysis of Security Algorithms in Cloud Com- puting", International Journal of Application or Innovation in Engineering Management (IJAIEM),Volume 3, Issue 3,On Page(s):171-176, March 2014.

[6] B. Sowmya Sri ;S.Vikramphaneendra; "A Secure Way for Data Storage and Forwarding inCloud", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 9, September 2013.

[7] Nivedita S.;Priya D.; "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", International Confer- ence on Computing Communication Control and Automation(ICCCA),On page(s):35-39,2015.

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

[9] Shweta S;,Manoj Kumar; "File Integrity Maintenance Tool for Secure Infor- mation Storage in Cloud", International Journal of Computer Applications (0975 – 8887)Volume 97– No.1,On page(s): 15-19,July 2014.

[10] Rashmi S. Ghavghave; Deepali M. Khatwar; "Architecture for Data Security In Multi-cloud Using AES-256 Encryption Algorithm", 2013 IEEE, Nirma Engineering(NUiCONE),On Page(s): 1-4.International Journal on Recent and Innovation Trends in Computing and Communication(IJRITCC),Volume: 3 Issue: 5, On Page(s):157 – 161,May 2015.

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

[12] 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.

[13] S.IShaik Hussain; V. Yuvaraj; "A SECURE DATA ACCESS CONTROL METHOD USING AES FOR P2P STORAGE CLOUD", IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICJJECS)2015,On Page(s):1-8,2015.

[14] 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.

[15] 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.