IJCSN International Journal of Computer Science and Network, Volume 4, Issue 4, August 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Hybrid Cryptographic Framework for Multimedia Data Storage over Cloud

[1] Ramandeep Kaur, [2] Gurjot Kaur

[1] Department of Computer Engineering
Chandigarh University, Gharuan

[2] Assistant Professor, Department of Computer Engineering
Chandigarh University, Gharuan

Abstract - Cloud computing environment gives various platforms, services and applications for better optimization of the data, scalability via storage and the cost reduction flexibility. It is the next era platform for acquiring the various services and platform without using them. We have worked on multimedia security with respect to multi media. Encryption algorithm AES and Elgamal is used for protection. Hybrids have been completed by using these algorithms. During Hybrid, the probability time has decreased while the probability used to increase when AES and Elgamal used. AES and Elgamal are primary used for multimedia purpose. Windows azure cloud situation is used to configure the data base. Our research aim is to give a state art knowledge to new inventors they would like to enter this motivating new region.

Keywords - *Computing, Multimedia Cloud, Data Storage, AES and Elgamal Algorithm.*

1.Introduction

The multimedia cloud computing from multimedia conscious cloud and cloud conscious cloud media vision [1]. Initially, the current a multi media conscious cloud, which addresses how cloud, can represent detached multimedia. A giving out and cloud storage space and present quality of service providing for multi-media services. Cloud computing is a service dispense over the internet for compute, data entrance and cloud storage space by create scalability, flexibility and reduce cost.[1, 2]. A cloud computing is one of the increasing information technologies used in computation now days. It is green technologies which agree to access; computing and storing the resources by offer variety services [2].The cloud computing is basically a type of computing that rely on allocation the computing resources and rather than local servers and applications. In cloud compute statement cloud used as a symbol for 'internet', so expression the cloud computing means "a type of internet based computing". The web tool services storage space and request are delivering to company computers [3].

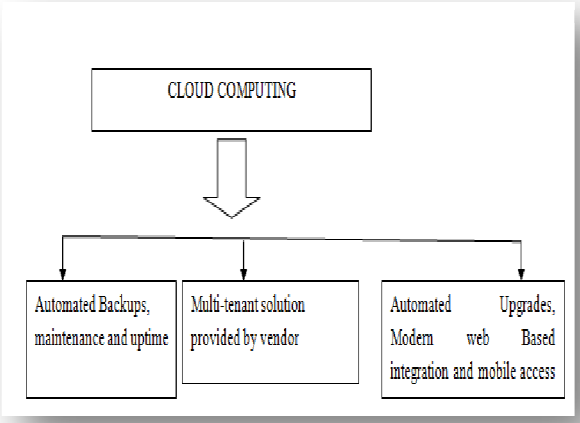

Figure : 1 Cloud Computing

In this, they are based on a very fundamental principal of 'reusability the IT capabilities'. They are difference that cloud computing brings comparing to the ancient ideas network computing, utility computing, distributed computing or spontaneous computing is to the broaden horizons across arrangement limits [4].

A. *Service Models:* A cloud is a compute process in which services are distributing over network using computation processes. The cloud symbol the hiding for complex environment it contains in system structure.Service models are three main grouping: SaaS, IaaS, and PaaS.

- *Software-as-a-Service:* The Software as services is high producing of a quality model. Where software hosted by the cloud venders are rented to the end client. They are replacing of the application running on pc. Who managed and hosted specialized business applications. Follow pay per use of example. Central organizations are reduced cost. In this, the sales force, Microsoft, yahoo, Google is offered by companies.

- *Platform-as-a-service:* The platform as services are refers to the software deployment framework, runtime environment and the element on pay to alter the direct readying of application level assets or internet application. It's a platform wherever package will be deployed, tested and residential. They are resources of entire life cycle are software can be operate on a PAAS.

- *Infrastructure as a service:* The hardware as services are also called the infrastructure as a service. They are provides computing capability as consistent services and basic storage over the network. A mutual and made available [4] to handle workloads are services, storage systems, networking tools, data centre space etc.

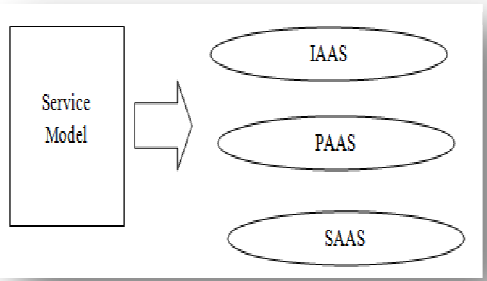

Figure : 2 Service Model

2. Multimedia Cloud Computing

Now a day's customers can simply access the multimedia content over the internet at any time. The user can efficiently store the multimedia substance of any type and any size in the cloud following subscribe it. Media is not storing the media like video, image and audio, its process them with the cloud because the computing time for processing media data is more difficult hardware. After the processing, process data can be received easily from the cloud through a user with no any requirement of adding difficult hardware [6]. Now a day's most of company's use clouds like azure, Google music, amazonEC2, Skype Driver and Drop box provide comfortable management/ organization system within the cloud network. The customers of these clouds can access the multimedia. For example, the user can view a video anyplace in the world at anytime using computers, tablets, laptops and Smartphone's.

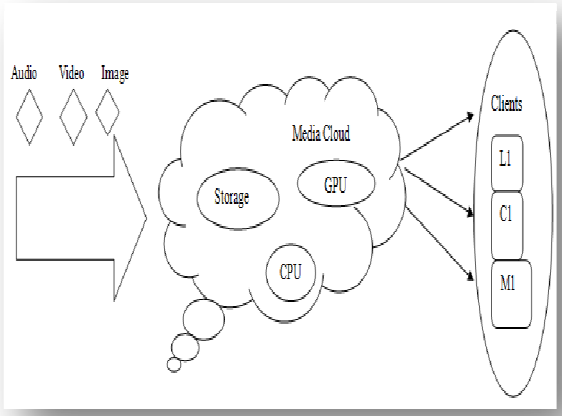

Figure : 3 Multimedia Concept

2.1 Cloud Media

A cloud has the multimedia satisfy of the vendor of that particular cloud. A media modify can be accessed although the multimedia protocols in the cloud computing and can be flowed to customers present in computers. Cloud gives a multi screen occurrence and gives the availability of media satisfies within it by abstraction the details and position of the satisfied on remunerated per needs. In case of media today's are engrossing more or a lot of sound, but quick development will be done on satisfied like movies [7], descriptions, e-mails and application etc. It gives a communications for integration media satisfy. It can servers as an interface for sharing the media satisfies the other smart devices like computers, tabs and mobiles app etc.

2.2 Cloud Media Services

A cloud gives a communications which agrees to visible access of data and store and process the data in a security purposes. Media is exchange from a public mechanism to cloud has altered the data partition model by its good organization evaluating with the past low secure data partition models. They give many benefits by losing the store challenges of public customer devices like computer, tabs, applications etc [8].

The additional variety multimedia cloud computing or cloud media services are:

- Cloud games
- Digital Image Processing

The multimedia cloud computing is a technology gives number of advantages to its services offers as well as the clients although more computation time, more efficient data storage capacity and cost reduce. It invented impact in the multimedia satisfies processing like store, encrypt, decrypt, compress and many more [9].

3. Cryptography

Cryptography is the Greek word "underground writing". It word refers to the art and knowledge of converting message to make the secure and resistant to assail [11]. They no one can refuse the vital of protected network and data communication. An essentially cryptography is based security in network. They are used for two texts. First is the plain text and second one is cipher text. The plain text is original message, previous transformed. The message is transformed after is called the cipher text.

Cryptography is two types:

- Symmetric key(is called secure key)
- Asymmetric key(is called public key)

A. *Symmetric Key:* The secret key is also called symmetric key. The together parties are used the similar keys. An Encryption algorithm to encrypt the data and the sender uses this key, same key use the receiver and the corresponding decrypt the message or data using decrypt algorithm. It mainly used in network protection is symmetric [10] key cryptography.

Types of Symmetric algorithms are:

- AES
- DES
- 3DES
- RC5
- BLOWFISH

AES: This is basically a symmetric chunk chiper. It uses the same key for both encryption and decryption. This algorithm provides a diversity of block key and key size not only the 64-bit and 56-bits of DES block and key size.

The AES algorithm standards position that the algorithm can receive a block size of 128-bits and a select of three keys: 128, 224 and 256 bits [10].

Algorithm:

STEPS:

Key Expansions—round keys are consequent from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

1. first Round

Add Round Key—each byte of the state is mutual with a block of the round key using bitwise xor.

2. Rounds

Sub Bytes—a non-linear replacement step where each byte is replaced with another.
Shift Rows—a transposition step where the last three rows of the state are shifted regularly a certain number of steps.
Mix Columns—a mixing operation which operate on the columns of the state, combining the four bytes in each column.
Add Round Key.

3. Last Round (no Mix Columns)

Sub Bytes
Shift Rows
Add Round Key.

B. *Asymmetric key:* An asymmetric key is used the two different keys public key and private key. The private key is kept by the receiver and public key is announced to the public.

Asymmetric algorithms are:

- RSA
- DSA
- DIFFIE-HELLMAN
- ELGAMAL

Elgamal Algorithm: The elgamal algorithm is a public key crypto based on the mathematical problem. It consists of both the encryption and signature algorithms. Basically encryption is not same as signature verification. Signature creation depends on the Elgamal algorithm. The main disadvantage of elgamal is required for randomness and c slower speed [11, 12].

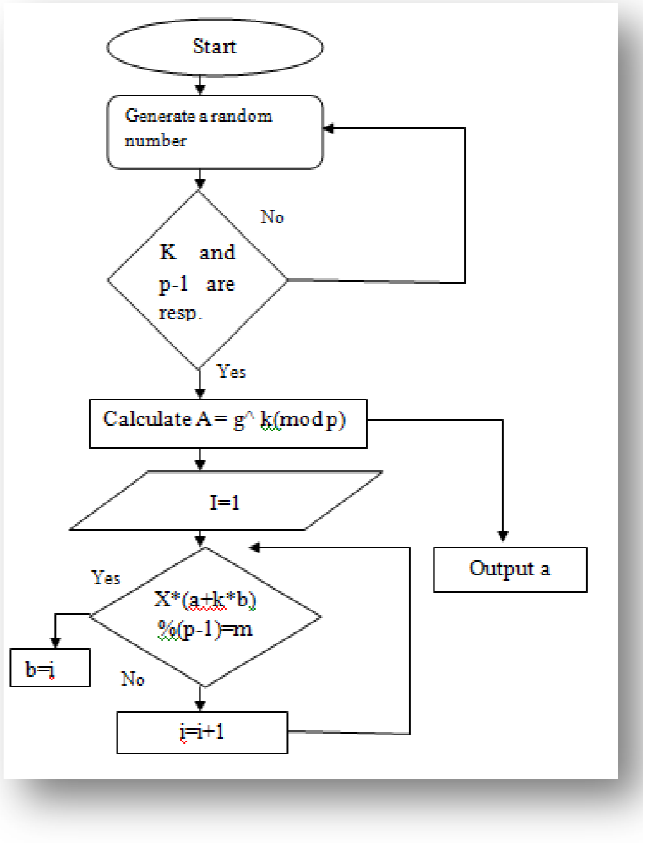

Figure : 4 Elgamal Algorithm Steps

4. Simulation Model

Initially, it is the first step that initializes whole process. When program starts it loads pages of system into memory to start process of encryption and call next step for uploading file into system. An Upload file, here user can upload files for encryption. Text, Audio, Video and Image, There are four types of files Text format, audio, video and Image. These files are used for encryption. Apply Elgamal, It used to generate key for encryption of data file. System configures it and uses their key for AES for encryption. Cipher Block, in this step cipher block of AES is generated with Elgamal key. And transfer control in two separate blocks of code 1. Mail system and 2. Encryption blocks AES. Mail Services, It is provided by gmail.com with SMTP protocols to attach system with Gmail server. It uses simple mail transfer protocol. After connecting system with Gmail, mail is sent to user with content as key. Encryption with AES, in this step AES encryption technique is applied on data with key and encrypts it for storing in database. Generate data, after applying both encryption algorithms, data is generated. It is encrypted data that is ready to store in database. All encrypted bytes are combined with each other to generate single file. Signature, Now add signature in the data to make it secure from external misuses. It is a digital signature that is used to upgrade the security content. An Upload, Here whole encrypted data is uploaded in database for further use. User, User can select file and can download file from the system. For this user requires key and signature to decrypt the file. The Key+ Signature, User enters the key that he has fetched from mail and signature that is entered at the time of uploading file. Download, If the key and signature are same than it will decrypt file, else the process of download is rejected by the system and ask from user to try again with other correct key and signature.

5. Methodology

Purposed Algorithm:

Step1. System.file.Upload (Image,Audio,Text,Video) This is the first step which used to get input from user. The input should be any kind of file which is as text file, audio file, video file or any image.

Step2. System. check(file.status)

System checks file status that file present or not. If it uploaded it shows status as true.

Step3. If(file.status.exist==false)

It compare system's file status that status true or false. If file present its status true otherwise it will false.

Step4. Repeat step(file. Upload)

Its transfer control for first step if the file status would be false. It shows that file not present. So it needs to show message for upload a file for further operations.

Step5. else { Data.mode.set==cipher }

Step6. algo. Elgamal. Prepare=true.

This step allows code to change working mode to cipher mode to apply encryption scheme. It used to initialize encryption on file.

Step7. Elgamal.generate.key=true.

First step to initialize Elgamal algorithm for key generation which require for encryption and decryption.

Step8. Cipher. Block =Elgamal. Key

Next step is also used to define blocks of data to be encrypts. It used to Encrypts key in data with using AES algorithm.

Step9. SMTP. Google. Services();

Step ninth are used to configure gmail with our system. This process use SMTP protocol for configuration.

Step10. Mail. Content(Key. Elgamal. Key());

Step tenth are used to configure gmail with our system. Here system uses this service for mail key to user for security purpose. System accepts digital signature for enhance security. It would be as image file for data security.

Step11. System. Encryption. Mode=Mode.AES;

Next three steps used to encrypt data block by block with using key. It generates encrypted data and embed key block wise.
Step12. If (key. Elgamal. Key () !=null) { AES.(Elgamal. Key. Content()) };
Step13. Data.Bytes.Encrypt(AES.Encryption)
Step14. Data(Add. Signature(Digital));
Data is combination of cipher bytes, Elgamal Key and digital signature. The whole bytes are combined and system generates output as encrypted data.
Step15. Data=Data()+Elgamal. Key ()+ Digital. Signature();
Data is combination of cipher bytes, Elgamal Key and digital signature. The whole bytes are combined and system generates output as encrypted data.
Step16. Encrypted _output_ Data = Data.
Steps17. Stop
Stop save all the data object and render page for further process. It unloads objects after rendering process would be complete and give response to user accordingly.

6. Experimental Results

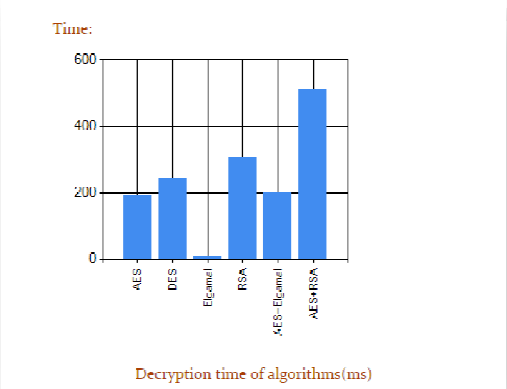

Figure : 8 Time consume

The above figure shows the time consumer graph. In this graph is show the consumer time different algorithms like AES, DES, ELGAMAL, RSA, AES+ELGAMAL and AES+RSA.

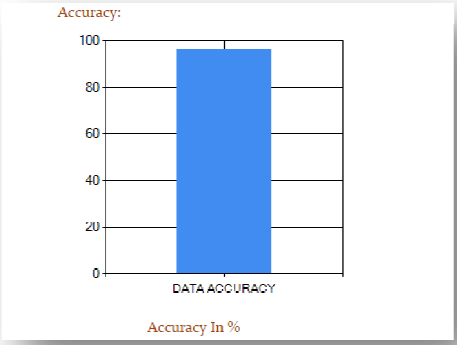

Figure : 9 Accuracy in percentage (%)

The above figure shows the accuracy graph. In this graph are show the accuracy in AES+Elgamal algorithm.

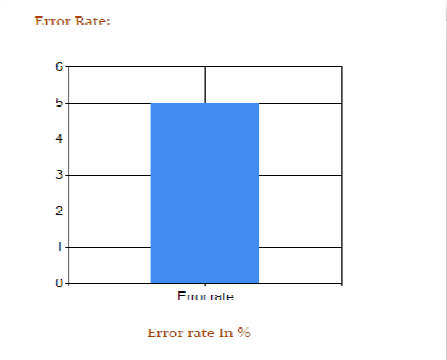

Figure : 10 Error rate in percentage (%).

The above figure shows the error rate.

7. Conclusion and Future Scope

In this thesis, various security concerns of cloud computing has been thoroughly examined. All the primary concerns of the data security namely privacy, verification and reliability have been addressed within in a single environment. The main motive behind this research is to propose a solution to secure the multimedia data storage and management since storage over cloud takes place somewhere at a location which is beyond data owners' domain of control. Apart from designing the planned solution, its completion is also done using Dot Net framework over Microsoft Windows azure server. Furthermore, in order to reproduce the optimal efficiency of this composite platform in comparison to their individual counterparts, performance analysis has been done on the basis of average execution time, accuracy etc. Thus, from the analysis, we finish here that the proposed

framework results in an optimal behavior in terms of confidentiality, encryption and accuracy. Our future work will be considering some difficulties regarded to accessible security algorithms and design a good versions of DES, 3DES, IDES and BLOWFISH. The proposed solution is implemented at a very smaller level where only a small amount of data is being outsourced to cloud.

References

[1] Danpeng, Sun, et.al. "The design and implementation of multimedia teaching platform in the cloud computing environment." Advanced Research and Technology in Industry Applications (WARTIA), 2014 IEEE Workshop on.

[2] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE,2009.

[3] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In Services,Computing,IEEE International Conference on, page 517520, 2009.

[4] Ma, Changsha, and Chang Wen Chen. "Secure media sharing in the cloud: Two-dimensional-scalable access control and comprehensive key management." *Multimedia and Expo (ICME), 2014 IEEE International Conference on*. IEEE, 2014.

[5] Wu, Y.; Zhuo, W.; Deng, R., "Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks," Multimedia, IEEE Transactions on , vol.15,no.4, pp.778,788, June 2013.

[6] Zhu, W.; Luo, C.; Wang, J. ; Li, S., "Multimedia Cloud Computing," Signal Processing Magazine, IEEE,vol.28, no.3, pp.59,69, May 2011.

[7] Zhu, X.; Chen, C. W., "A collusion resilient key management scheme for multi-dimensional scalable media access control," Image Processing (ICIP), 2011 18th IEEE International Conference on , vol., no., pp.2769,2772, 11-14 Sept. 2011.

[8] Bethencourt, J.; Sahai, A.; Waters, B., "Ciphertext-Policy Attribute-Based Encryption," Security and Privacy, 2007. SP '07. IEEE Symposium on , vol., no., pp.321,334, 20-23 May 2007.

[9] Altamimi, Majid, et al. "Energy-as-a-Service (EaaS): On the efficacy of multimedia cloud computing to save Smartphone energy." *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*. IEEE, 2012.

[10] Kang, Li-Wei, et al. "Privacy-preserving multimedia cloud computing via compressive sensing and sparse representation." *Information Security and Intelligence Control (ISIC), 2012 International Conference on*. IEEE, 2012.