SECURITY FOR MULTIMEDIA CONTENT IN CLOUD USING DOUBLE ENCRYPTION

Komal.D.Jadhav [1], Jogendra.N.Nandanwar [2], Shankar.M.Patil[3]
BE Students[1,2], Associate Professor[3]
Department of IT
Bharati Vidyapeeth College of Engineering, Navi Mumbai, India

Abstract: There Abstract— the cloud computing offers high scalability, confidentiality and the easy accessibility of the information over the Internet. Though the conventional encryption system provides security, the most concerned issue is the regular side channel attack for capturing ones sensitive and confidential image, audio and video. A malicious Virtual Machine (VM) besides a targeted VM can extract all information. Thus, this paper implements a double stage encryption algorithm for multimedia content security using random key generation approach. The first stage encrypted multimedia content into cipher text-l using a symmetric public key. The cipher text-l is again encrypted in the cloud using a randomly generated asymmetric private key. If anyone gets the cipher text, he could not extract the encryption key to recover the multimedia contents.

Index Terms **- Cloud Computing, Multimedia Security, Double Encryption & Decryption.**

I. INTRODUCTION

Cloud computing is the freedom of processing and storing data of the consumers in a third party data centre using the remote computing resources over the Internet. Rather than keeping files on a hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. With the help of internet access, it allows consumers and businesses to use applications without installation and access their personal files at any computer. The consumers need no concern where the hardware and software or the application is operating, they only need to have a simple device that can simply operate with the cloud. The consumers pay much less for the cloud and have no maintenance liabilities.

In IaaS, the cloud provider supplies Virtual Machines (VMs) and storage on which consumers can build and run applications. Virtual Machines (VMs) are a set of virtualized infrastructural components.[1] The PaaS offers third party services like operating system, programming environments and web servers, whereas SaaS offers different application software. The four popular cloud deployment models for the consumers are: private cloud, public cloud, hybrid cloud and community cloud. Public cloud environments are accessible by multiple renters, whereas the private clouds are decorated with virtual resources for particular organization only. Hybrid cloud is the composition of public and private cloud and community cloud is dedicated to several groups.

The private cloud is protected by that particular organization, the rest have data risk and security issues.[2] Moreover, cloud preserves these data and multimedia contents to a large data centre.[3] A third party manages the data centre and has the liabilities to make certain security for the protection of the data and multimedia contents and provide uninterrupted services. Unless there may arise a security question and trustworthiness of third party. [4] The side channel attacker extracts the data or multimedia contents after placing a malicious VM beside the targeted VM. [5]

The most dealing issue is the security of the cloud, especially the data and multimedia contents such as image, audio and video. Several studies have been done on the security of the multimedia contents in the cloud and decrease the side channel attack. [6] These studies focused on the combination of two different algorithms and generate a security key for consumers as a key to access the cloud. These drawback let us to implement a double stage encryption algorithm for the security of multimedia contents against a negligent third party and side channel attack.

For the security of multimedia contents this paper implements a double stage encryption algorithm using a randomly generated key and the 94 bit converter. The remarkable feature of the randomly generated key makes the second stage encrypted data unbreakable. Thus, the paper provides more security of the multimedia content in the cloud.

II. LITERATURE SURVEY

This section describes a literature review, to find out an effective algorithm having widely applicable cloud security for the multimedia contents against the side channel attack. Priyanka V. Padwal et al [7] this paper described about multimedia content protection on cloud infrastructures. The system runs on private clouds, public clouds, or any combination of public-private clouds. The aim of this paper was for protecting multimedia content, which content-based copy detection (CBCD). In this approach, signatures are

extracted from original data objects. The goal of the proposed system for multimedia content protection is to find illegally made copies of multimedia objects over the Internet.

Priyanka Gupta et al [8] This paper explains a new method which is a combination of (RBAC)Roll Based Access Control with a combination of RSA and blowfish , signature verification to enhance security when storing multimedia data onto cloud server. An efficient framework is proposed to provide data storage in the cloud environment with secure user cloud security. In this framework a secure three tier architecture is presented in which original file (text, audio, video, image) is stored on local server, the encrypted filename and the description of the original file is stored on cloud server, and to decrypt the file user has to enter private key which is stored in its Gmail account. This will enhance security as if the hacker hacks the local server he will only get original file ,if he hacks the cloud server he will get only the description and not the original file and to decrypt the file he will have to hack the Gmail server.

Chaya M et al [9] in this system the detection of duplicated content is done using cloud system environment, the content copyright is checked of the material in the environment. It handled various multimedia data such as text, images, audio and video. The signatures are detected from the multimedia objects from system abstracts. The creation and comparison of signature is different for specific media and other parts of the system does not depend on media type. Two components of the system are proposed. The two methods are first is creating signature for multi data and the second one is for matching the media objects by distributed index.

Rao, D et al [10] in this the multimedia image transfers is done using multi-layered security. It would enable the users among the globe to share the encrypted files wirelessly through http. When the image will get captured it will get encrypted with the 'AES' algorithm inside the device with the merged password that will be sent to the sender's cloud account password.

IV. PROPOSED SYSTEM

In this paper, the implementation plan performs the better security for multimedia data against side channel attack in cloud computing. The whole process is shown in the block diagram in Fig. 1. The double stage encryption and decryption process was done for cloud security. The multimedia contents are encrypted at the first stage by the conventional encryption process (AES, RSA) using symmetric key. In the second stage, the encrypted cipher text-l is then again encrypted by the randomly generated asymmetric key thus produce ciphertext-2. In the decryption stage, the encrypted ciphertext-2 is decrypted by the asymmetric key in the first decryption process. Thus produced the cipher text-I. The cipher text-l is then decrypted by symmetric key method (AES, RSA) and regain the original multimedia content. Since in the conventional encryption process the key is symmetric the attacker can easily be access the encryption key and retain original multimedia content. In the proposed encryption method the key is generated randomly and the Key exposition possibility is low.

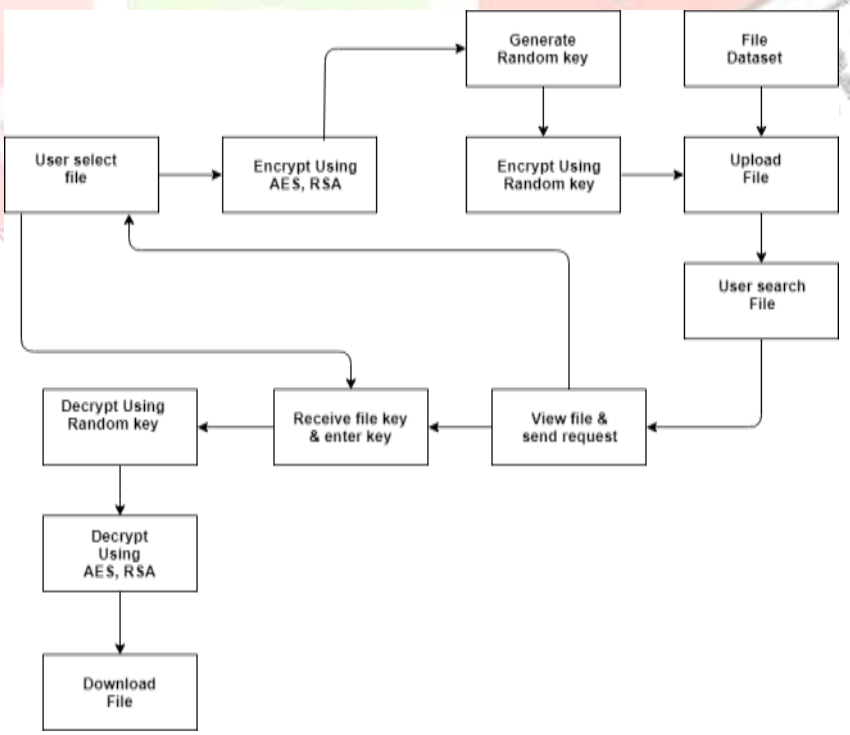

Fig.1. Block Diagram of Proposed System.

3.1 File Dataset

The first block of the proposed system implies the files and data can be uploaded, downloaded and shared through the cloud. The data can be a text file, a document, and audio, video file**.**

3.2 Upload file

The user can upload the file which the user wishes to store on cloud, for uploading the file the user will have to first login and then can upload the file from the option.

3.3 View file & Send request

After the user login various options are made available such as view file, share file, upload and download file. The view files shows the files that are shared and uploaded.

The user can send the request for sharing the file to another user, the decryption key is send to the user via the mail id provided during the registration.

3.4 Receive file key & Enter key

As discussed above the user receives a mail id in which the decryption key is given and then the key has to enter to fulfil the request.

IV. IMPLEMENTATION

4.1 Encryption process

In encryption process the actual data in converted into cipher text 1 which is stored in a file, which will be used for the second encryption to generate cipher text 2 .A randomly generated asymmetric key is used for the cipher text 2 encryption , then the data is stored in the cloud.

In the first encryption process, the multimedia data is converted into cihertext-1 using public symmetric key. Then for the second encryption process, a random prime number (p) is chosen. The cipher texts are read character by character. In each pass a single character (n) is multiplied with the prime and converted the result into (m) to the 94-bit format. The converted value is then stored in the cloud. A separator is then added with that value. The 94-bit format is the set of printable character having the ASCII value from 33 to 126. To prevent from generating the next prime location from out of range, the prime number (p) is mod by the character (n) and stored the result as (s). The location of the next random prime is the lower index of the mod result (s). A prime array is used to generate the random prime. On the second pass the prime array is rearranged by moving the prime number onto the first location of the array. The procedure ensures that selected prime is always random. With every pass of the encryption process the separators are programmatically generated that will help to find the random prime at the time of decryption. Until remaining the ciphertext-2 the procedure is continued.

4.2 ENCRYPTION-PROCEDURE (String str)

```
1 len := str.length
2 p := Random (prime)
3 for i=1 to len
4 n := str [i]
5 k := 94-bit-converter (p*n)
6 PRINT "k" II k as a cipher text
7 s := p mod n
8 p := s-1
9 end
```

After completing the whole encryption process of the ciphertext-1 into the ciphertext-2 the encrypted data is stored in the cloud.

4.3 Decryption process

In the decryption process at first, the cipher text each character is read sequentially one after another and add them to the temp (temporary variable) until found the separator. A character out of 94-bit converter is treated as a separator. By using the separator the random prime (p) is regenerated using at the time of encryption. Then the temp is converted into a decimal value (v). The value is then

divided by the prime (p) and regained the desired ciphertext-1 (n). The cipher text- 1 is then stored in the temporary string until the cipher text- 2 remains. The desired output strings are then written to the targeted file and stop the decryption process. Again decrypting the ciphertext-1 for the second step the multimedia data is finally recovered

4.4 DECRYPTION-PROCEDURE (string cp)

```
1 len := cp.length
2 t := charValue (cp [0])
3 p := prime [t-l ]
4 for i= 0 to len - 1
5 set k := cp [i]
6 if separtor == false
7 temString := temString + k
8 else v := temString
9 n := vip;
10 str := str + n
11 temsSring := NULL
12 t := upperPos (p mod n)
13 p := prime [t-l]
14 end
15 return str
```

4.5 AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network.

1. Key Expansions—round keys are derived from the cipher key using AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round
   a. Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
   a. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

   a. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   b. Add Round Key
4. Final Round (no Mix Columns)
   a. Sub Bytes
   b. Shift Rows
   c. Add Round Key.

4.6 Random Key Generation Approach

The cloud is a server-client model and the server system consists of agent module, security module, analysis module and database. Though the conventional cloud model has single encryption and decryption process, the proposed cloud security model has double encryption and decryption model. In the security module, the content manager introduces the cloud contents double encryption processes (Encryption I and Encryption 2).

The Encryption-I is usually provided by all cloud architecture and produces cipher text-I, the proposed Encryption- 2 is an attachment based on the architecture in paper to secure the cloud data using randomly generated key and convert the cipher text-I into ciphertext-2. The randomly generated key is unknown to the content manager too. In the client, the decrypt processor has double decryption processes (Decryption-l and Decryption-2) and content player.

The proposed Decryption-I is decrypted by random key and converts the ciphertext-2 into cipher text-I. The Decryption- 2 finally converts the cipher text-I to multimedia contents using symmetric key. Without the randomly generated key, the Decryption-I process is difficult and thus the proposed architecture gives efficient security.

This explains the result of proposed approach through the multimedia setup to secure the data in the cloud server. Different size various data, different data size takes different time to generate ciphertext-1 and 2. The analysis is shown for different data size which will provide the hopeful tests for various formats and sizes.

ITEM NO.	IMAGE (MB)	AUDIO (MB)	VIDEO (MB)
1	0.05	1.24	1.25
2	0.25	1.45	1.45
3	0.34	1.80	1.65
4	0.40	2.30	1.85
5	0.64	2.45	2.25
6	0.70	2.65	2.56
7	0.84	2.74	2.86
8	1.00	3.00	3.25
9	1.25	3.15	3.45
10	1.30	3.24	3.84

Table.1.Different types of media data.

V. CONCLUSION

A double stage encryption algorithm that provides the security of multimedia contents in the cloud. The proposed algorithm is crucial in the second stage. At first, the multimedia content stored in a file. The file is encrypted in cipher text-l after executing the Java code in Eclipse. The cipher text-l is stored in another file. Second, this file is encrypted again using a randomly generated key and the 94 bit converter into the cipher text- 2 after executing the Java code in the cloud or virtual machine. The decryption process is at the same but in reverse order that have done before for the encryption process. The proposed algorithm protect the information from the side channel attacker to grab the multimedia data into the cloud. Thus, the multimedia content is safe in the cloud.

REFERENCES

[1] w.kim, "Cloud Computing: Today and Tomorrow." Journal of object technology, vol. 8, no. 1, pp. 65-72, 2009.

[2] H. Takabi, 1. B. Joshi, and G.-J. Abn, "Security and Privacy Challenges in Cloud Computing Environments;' IEEE Security & Privacy, no. 6, pp. 24-31, IEEE, 2010.

[3] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation computer systems, vol. 28, no. 3, pp. 583- 592, Elsevier, 2012

[4] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond Lightning: A Survey on Security Challenges in Cloud Computing;' Computers & Electrical Engineering, vol. 39, no. I, pp. 47-54, Elsevier, 2013.

[5] L. M. Kaufman, "Data Security in the World of Cloud Computing," IEEE Security & Privacy, vol. 7, no. 4, pp. 61-64, IEEE, 2009

[6] Handbook of Modern Sensors (Physics, Designs, and Applications) by Fraden, Jacob.