Security in Multimedia Cloud Computing Using Encryption Algorithms: A Survey

Gemini Garg[1], **Jaspreet Kaur**[2]

[1]Chadigarh Engineering College, Landran

[2]Chandigarh Engineering College

Abstract: ***A multimedia cloud computing is a rising expertise developed for provided that various computing and storage services over the Internet. This paper performs an in depth survey on recent multimedia storage security study activities in organization with cloud computing. Past an overview of the cloud storage system and its security difficulty. Then it is explained the several key ideas and solutions planned in the present novel and point out possible extension and innovative research opportunity. This study purpose is to offer state of the art information to new researchers who would like to enter this moving new field.***

Keywords: Multi Media Security, Cloud Computing, Data Security, Access Control.

1. Introduction

Multimedia data is a group of some of the following medium: content, audio, moving image, and film. Multimedia protection deals with conduct of defensive such material .By using multimedia information, the multimedia data can be transfer from users having transferable devices such as changeable phones. Multimedia data escape having issues of the material rights and the privacy and therefore defensive the multimedia in sequence becomes critical in multimedia used devices [1]. Since large amounts of multimedia information hold vast sizes, we require a competent encryption technique for defensive the multimedia data at the same time as satisfying the simultaneous necessity.

2. Multimedia Data Security

Due to the current development in computer network technology, giving out of digital multimedia pleased through the internet is massive. Though, the augmented number of digital documents, compact disk processing tools, and the international ease of use of Internet access has created a very appropriate medium for exclusive rights fraud and disobedient distribution of multimedia content. A major condition now is to protect the scholar possessions of multimedia content in compact disk networks. There are figure of data types that can be characterize as multimedia data types

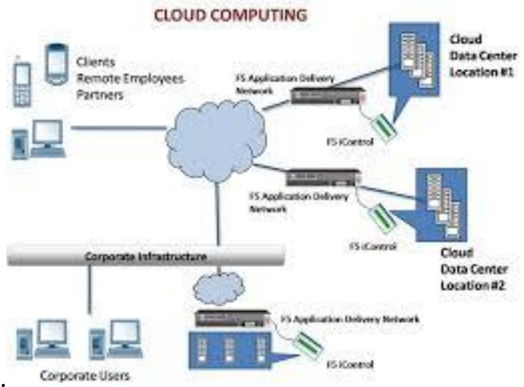

Figure 1: Cloud Computing

These are typically basics for the building blocks of general multimedia environments, platform, or integrate tools [2]. The essential type can be described as text, images, audio, video and Graphic objects. Multimedia finds its purpose in various areas counting, but not limited to, advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications.

The basic building of a cloud storage system is calm by a storage resource pool, including the distributed file system, the Service Level Agreements, and service interfaces [3]. Moreover, the structural design can be decayed into five layers based on their logical function limits as shown in Fig. 2

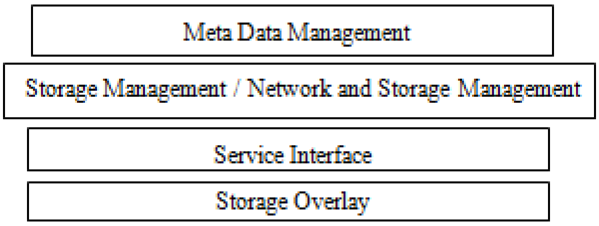

Figure 2: Cloud storage layered model [3]

3. Multimedia Data

There are number of information sorts that can be described as interactive media information sorts. These are commonly the components for the building squares of mineral summed up mixed media situations, stages, or coordinating apparatuses [4]. The essential sorts can be depicted as takes after:

- **Text:** The structure in which the content can be put away can shift enormously. Notwithstanding ASCII based documents, content is commonly put away in processor records, spreadsheets, databases and annotations on more broad media objects. With accessibility and expansion of GUIs, content textual styles the employment of putting away content is getting to be complex permitting enhancements (shading, shades...).

- **Images:** There is awesome difference in the quality and size of capacity for still pictures. Digitalized pictures are succession of pixels that speaks to an area in the client's graphical showcase. The prominent picture arrangements are jpg, png, bmp, and tiff.
- **Audio:** An undeniably well-known information sort being coordinated in the greater part of uses is Audio. It's truly space concentrated. One moment of sound can take up to 2-3 Mbs of space. A few strategies are utilized to pack it in suitable arrangement [5].

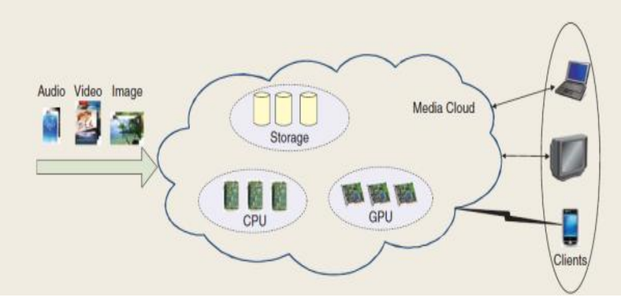

Figure 3: Fundamental concept of multimedia cloud computing

4. Security Threats in Multimedia

a) **Inside assaults**
There is plausibility for phishing and taking of media substance by the representative of the administration supplier itself.

b) **Legal and theft troubles**
There are more legitimate troubles on account of putting away media content in the web outside the limit i.e. Servers which are outside the nation. Likewise there are limitations in getting the media substance rights for diverse stages and imparting the media content outside the extent or utmost.

c) **Migration**
The client may think to move all his media substance to some other spot taking into account his adjustment in prerequisites. In any case, now the client does not have the opportunity of doing that [6].

5. Advantages of Multimedia Data Security

Media equipment offers number of key remuneration to its examine provider as well as the users from side to side enlarged completion time, well organized data storage capacity, less calculation and cost [7]. Some more recompense is described below:

- **Cost**
Media compute offer cost effective military to its service provider through efficient multiplexing of media inside like audio, video, image by as long as a common infrastructure, utilize the server, optimization, virtualization, Mobility and habitual processing. There is no requiring for actually acquiring a communications or reserve in our local system and thus reduce the cost [8].

- **Compatibility**
Media allow the medium satisfied to be access anywhere through any smart mechanism and it is [9].

- **Storage**
Media knowledge has many bases for store the media content using the income. Also it is more sheltered since the store media contented will be duplicate without manual intrusion.

6. Disadvantages of Multimedia

1. Expensive
2. Not always easy to configure
3. Not only Compatible [9]

7. Cloud Computing Characteristics

a) Large Scales*:* "Cloud" gives users an unprecedented computing capacity.

b) **Virtualization:** Cloud computing allows users at any location, using a variety of terminal access to application services. The requested resources from the "cloud" do rather than fixed physical entity. Application in the "cloud" somewhere in the running, but in fact users do not know or worry about the specific location of running applications.

c**) High Reliability** "Cloud" of data using multiple copies of tolerance, computing nodes are interchangeable with the structure and other measures to ensure the service reliability, the use of cloud computing and reliable than using the local computer.

d) High Scalability: "Cloud" the size of dynamically scalable to meet the growing size of applications and user needs.

e) On-demand Service: "Cloud" is a huge resource pool, you can purchase on demand; clouds can follow flow of the billing [10].

8. Existing Algorithms For Security

To present secure message over the network, encryption algorithm plays a vital role. It is the primary tool for defensive the data. Encryption algorithm converts the data into twisted form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data [11].

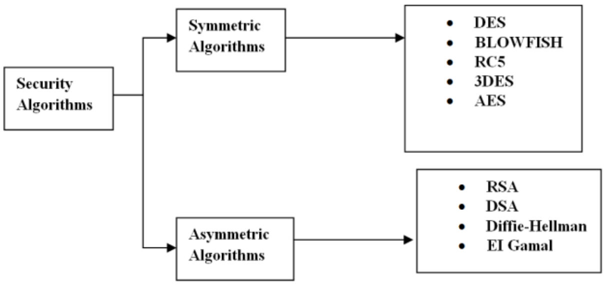

Figure 4: Security Algorithm

4.1 Symmetric Algorithms

a) DES: This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be optional by National Institute of Standards and Technology. DES is 64 bits key size with 64 bits block size. Because that time, many attacks and method have witnessed weakness of DES, which made it an unsure of physically block cipher [12].

ALGORITHM:

```
Function DES_Encrypt (M, K) where M = (L, R)
M ← IP (M)
For round ←1 to 16 do
Ki ←SK (K, round)
L ←L xor F(R, Ki)
Swap (L, R)
End
Swap (L, R)
M ←IP-1(M)
Return M
End
```

b) Blowfish: This was developed in 1993. It is one of the most ordinary public algorithms provide by Bruce Schneider. Blowfish is a changeable length key, 64-bit block cipher. No attack is recognized to be successful against this. Various experiment and research analysis proved the advantage of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power expenditure.

ALGORITHM

```
Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
XL= XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Next i
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR
```

c) **RC5**: It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The velocity of this algorithm is slow.

ALGORITHM

```
A = A + S[0];
B = B + S[1];
for i = 1 to r do
A = ((A Xor B) <<< B) + S[ 2 * i ]
B = ((B Xor A) <<< A) + S[ 2 * i + 1]
Next
```

Table.1 Comparison Table

Algorithm	Comparison
DES	ES has key Size of 64 bits.
Blowfish	CAST-128 has block size of 64 bits.
RC5	RC6 has Key size and Block size of 128 bits.

9. Conclusion

It is required for the cloud storage to be able to with storage security solution so that the whole cloud storage space system is consistent and reliable. This work, conduct a concise survey on a set of newly available papers and describe some hot study topics in greater detail, including data integrity, data confidentiality, access control, data manipulation in the encrypted data domain, etc. As the unusual nature of multimedia data, it based on cloud computing purpose leaning database of such a instrument just to satisfy the media database model requirements. Even if it has many theoretical and practical harms be solved with the perfect the cloud based entity oriented multimedia database for its unique advantages, will become the conventional of the development of multimedia database.

References

[1] A. Francia III, M. Yang, and M. Trifas “Applied Image. Processing to Multimedia Information Security,” IEEE, 2009.

[2] B. Furht, D. Socek, and A. M. Eskicioglu, “Fundamentals of Multimedia Encryption Techniques,” CRC Press, 2004.

[3] W. Zeng, Y. Zhao, K. Ou, and W. Song, "Research on cloud storage architecture and key technologies," in Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009, pp. 1044-1048.

[4] B. Furht and D. Kirovski, “Multimedia Encryption Techniques and Applications,” Auerbach Publicationspp.91–128, 2006.

[5] T. B. Maples and G. A. Spanos, “Performance study of selective encryption scheme for the security of networked real-time video,” in Proceedings of the 4th International Conference on Computer and Communications, Las Vegas, NV,1995.

[6] L. Tang,” Methods for Encrypting and Decrypting MPEG Video Data Efficiently,” in Proceedings of the 4th ACM International Multimedia Conference, Boston, MA, 2006.

[7] L. Qiao and K. Nahrstedt, “A New Algorithm for MPEG Video Encryption,” in Proceedings of the 1st International Conference on Imaging Science, Systems and Technology (CISST ’97), Las Vegas,NV, pp. 21-29,1997.

[8] B. Bhargava, C. Shi, and Y. Wang, “MEPG Video Encryption Algorithms”, 2002, Available:http://raidlab.cs.purdue.edu/papers/mm.ps

[9] C.-P. Wu and C.-C. J. Kuo, “Fast Encryption Methods for Audio visual Data Confidentiality,” SPIE International Symposia on Information Technologies 2000, Boston, MA, pp. 284-295, 2002.

[10] Zhang Mian et.al,” The Study of Multimedia Data Model Technology Based on Cloud Computing”, 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[11] Peng, B., Cui, B., Li, X.: Implementation Issues of A Cloud Computing Platform. IEEE Data Eng. Bull. 32(1) (2009) 59{66.

[12] Kaur, Randeep, and Supriya Kinger. "Analysis of Security Algorithms in Cloud Computing."