International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Security and Privacy in Multimedia Content in Cloud Computing

Mysagalla Mahesg
Adavelli Ramesh
Machukonda Kishore
Mtech (CSE)
Asso. Prof & HOD(CSE)
Assit. Prof. & Mtech(CSE)
SLC's College of Engineering and

ABSTRACT

To provide rich media services, multimedia computing has emerged as a noteworthy technology to generate, edit, and search media contents, such as images, graphics, video, audio, and so on. For multimedia applications and services over the Internet and mobile wireless networks, there are strong demands for cloud computing because of the significant amount of computation required for serving millions of Internet or mobile users at the same time. This paper reviews brief literature on multimedia cloud computing aspects and describe some of the security issues in cloud computing, including data integrity, data confidentiality, access control, data manipulation in the encrypted data domain, with respect to the existing security algorithms.

KEYWORDS

Cloud Computing, Multimedia, Internet.

I. INTRODUCTION

There are a number of data types in use today that can be characterized as multimedia data types. These are the elements used for the building blocks of other generalized multimedia environments, platforms, or integrating tools. The basic types can be described as follows:

- **Text**: The form in which the text can be stored can vary greatly. In addition to the ASCII based files, text is typically stored in processor files, spreadsheets, databases and annotations, on more general multimedia objects. With availability and proliferation of GUIs and text fonts, the job of storing text is [9] becoming complex allowing special effects (color, shades...).
- **Images**: There is great variance in the quality and size of storage for still images. Digitalized images are sequence of pixels that represents a region in the user's graphical display. The space overhead for still images varies on the basis of resolution, size, complexity, and compression scheme used to store image. The popular image formats are jpg, png, bmp, tiff.
- **Audio**: An increasingly popular data type being integrated in most of applications is Audio. It is quite space intensive. One minute of sound can take up to 2-3 Mbs of space. Several techniques [10] are used to compress it in a suitable format.
- **Video**: One on the most space consuming multimedia data type is digitalized video. The digitalized videos are stored as sequence of frames. Depending upon its resolution and size a single frame can consume up to 1 MB. Also, to have a realistic video playback, the transmission, compression, and decompression of digitalized require continuous transfer rate.

II. MULTIMEDIA DATA IN CLOUD COMPUTING

As a result of the growing popularity of the cloud computing platforms, multimedia mails, orchestrated presentations, high-quality audio and video, collaborative multimedia documents and other rich media applications can be stored in the cloud data

storage server. This is utilized by an everyday increasing number of cloud users who can easily access the multimedia content over the internet at any time. The user can efficiently store the multimedia content of any type and of any size in the [3] cloud after subscribing it with no difficulties. Not only the storing of the media content like Audio, Video and Image, but can process them within the cloud since the computation time for processing media data is more in complex hardware. After processing the processed data can be easily received from the cloud through a client without any need of installing complex hardware. Thus Multimedia cloud computing is the processing, accessing [4] and storing of multimedia contents like audio, video and image using the services and applications available in the cloud without physically acquiring them. Multimedia processing in a cloud imposes great challenges. Several fundamental challenges for multimedia computing in the cloud are highlighted as follows.

1. Multimedia and service heterogeneity:

The types of multimedia and services, such as voice over IP (VoIP), video conferencing, photo sharing and editing, multimedia streaming, image search, image-based rendering, video transcoding [5] and adaptation, and multimedia content delivery, the cloud shall support different types of multimedia and multimedia services.

2. QoS heterogeneity:

For different multimedia services different QoS requirements should be include and the cloud shall provide QoS provisioning which support for various types of multimedia services to meet different multimedia QoS requirements.

3. Network heterogeneity:

The cloud shall adapt multimedia contents for optimal delivery to various types of devices with different network bandwidths and latencies which providing different networks, such as Internet, wireless local area network (LAN), and third generation wireless network, have different network characteristics, such as bandwidth, delay, and jitter .

4. Device heterogeneity:

As different types of devices, such as TVs, personal computers (PCs), and mobile phones, have different capabilities for multimedia processing; the cloud shall have multimedia adaptation capability to [6] fit different types of devices, including CPU, GPU, display, memory, storage, and power.

Currently many companies have introduced clouds like AmazonEC2, Google Music, DropBox, SkyDrive which provide content management system within the cloud network. The users of these clouds can access the multimedia content for example; the user can view a video anywhere in the world at any time using their Computers, tablets or smartphones.

Such rapid advances in broadband communication, high speed package switching network systems as well as the growing demand on multimedia file sharing have made effective multimedia data transmission and storage increasingly important. However, serious security issues arise in association with the expanding storage data center of the cloud server, which stores multimedia files of users such as personal photos and videos.

III. SECURITY ASPECTS IN CLOUD COMPUTING

A. Availability
B. Confidentiality
C. Privacy
D. Data Integrity
E. Identity and Access Management (IAM)
F. Control
G. Audit
H. Compliance

IV. SECURITY THREATS TO MULTIMEDIA

A. Inside attacks

There is a possibility for phishing and stealing of media content by the employee of the service provider itself.

B. Legal and piracy difficulties

Since the cloud media computation is very new, the legal standards are not very good. There are [7] more legal difficulties in the case of storing media content in the cloud outside the boundary i.e. Servers which are outside the country. Also, there are restrictions in getting the media content rights for different platforms and sharing the media content outside the range or limit.

C. Migration

Since more and more clouds are launched by the service providers, the user might think to move all his media content to some other cloud based on his change in requirements. But now the user does not have the freedom of doing that.

D. Challenges over standards

Currently many vendors (person who sellsservices) developing and launching their own private cloud environments based on their own conditions and security features which leads to issues in interoperability in the near future.

E. QOS

In cloud media computing, since it is a new area, the developers are concentrating more on computation speed and storage issue. Users going for unreliable networks without their knowledge to [8] share the media content even though there are availability of more promising streaming technology and increased broadband speed.

F. More confusion

There are more confusion among the user in choosing the type of cloud since both pay per use and free clouds are launched by some mobile companies, service providers etc. So the users face difficulty in taking a decision.

V. LITERATURE SURVEY

Sara Qaisar et al. [1] proposed Network/Security Threats and Counter Measures for cloud computing. Cloud computing improves organizations' performance by utilizing minimum resources and management support, with a shared network, valuable resources, bandwidth, software's and hardware's in a cost effective manner and limited service provider dealings. Basically it's a new concept of providing
virtualized resources to the consumers. Consumers can request a cloud for services, applications, solutions and can store large amount of data from different location. But due to constantly increase in the popularity of cloud computing there is an ever growing risk of security becoming a main and top issue. This paper presented the three models of the cloud, the network issues and the comparative study of implementing encryption algorithm for securing the cloud.

Alzaber et al.[2] discussed that multimedia file storage in cloud computing required the security. Multimedia cloud computing is termed as multimedia computing over grids, content delivery network (it is used for reduce the latency and increase the bandwidth of data), server-based computing, and P2P multimedia computing. It gives infrastructure of high-performance computing (HPC) aspect.

J.Nieh et al.[3] proposed that Desktop computing is Server-based multimedia computing addresses in which all multimedia computing is done in a set of servers, and the client interacts only with the servers.

Mr. Prashant et al.[4] described the use of Digital Signature and Diffie Hellman Key Exchange blended with AES algorithm to protect confidentiality of data stored in cloud. Even if the key, which is confined to legitimate user, got hacked the facility of Diffie- Hellman key exchange renders it useless. The three way mechanism architecture made it tough for the hackers to crack the security system thereby protecting the data stored in cloud.

Somani et al. [5] assessed cloud storage Methodology and Data Security in cloud by the implementation of digital

signature with RSA algorithm.

Fusenig et al. [6] proposed a new approach called cloud networking adds networking functionalities to cloud computing and enables dynamic and flexible placement of virtual resources crossing provider borders. This allows various kinds of optimization, e.g., reducing latency or network load. However, this approach introduces new security challenges. This paper presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in the cloud networking infrastructure.

Dean Chen et al. [7] provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.

VI. PROPOSED SOLUTION

A major requirement is to protect the intellectual property of multimedia content in multimedia networks. The problem revolves around the Cloud security and the appropriate implementation of cloud over the network. Thus,

- In order to keep user's data secure on cloud, a data encryption using Advanced Encryption Standard (AES) algorithm and elgamal algorithm can be implemented.

This multimedia security problem would be solved by using the combination of AES and Elgamal algorithm, earlier research has been done in this field, yet a lot can be done.

VII. CONCLUSION

There are various solutions proposed to ensure cloud storage security, including certification, authority, audit and encryption in last several years. It is essential for the cloud storage to be equipped with storage security solutions so that the whole cloud storage system is reliable and trustworthy. In this paper, we conducted a brief survey on multimedia cloud computing aspects and described some security issues in cloud computing, including data integrity, data confidentiality, access control, data manipulation in the encrypted data domain, etc along with security algorithms. An encryption based solution has also been proposed to attain data storage security.

REFERENCES

[1] Sara Qaisar and KausarFiaz Khawaja, " Cloud computing : network/security threats and countermeasures," ijcrb, vol. 3, no.9, January 2012.

[2] B. Aljaber, T. Jacobs, K. Nadiminti, and R. Buyya, "Multimedia on global grids: A case study in distributed ray tracing,"Malays. J. Comput. Sci., vol. 20, no. 1, pp. 1–11, June 2007.

[3] J. Nieh and S. J. Yang, "Measuring the multimedia performance of server based computing," in Proc. 10th Int. Workshop on Network and Operating System Support for Digital Audio and Video, 2000**,** pp. 55–64.

[4]. Mr. PrashantRewagad, and Ms.YogitaPawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," 978-0-7695-4958-3/13 $26.00 © 2013 IEEE.

[5] Uma Somani, Kanika Lakhani, and Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[6] Volker Fusenig and Ayush Sharma "Security Architecture for Cloud Networking," 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.

[7] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing," 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[8] Farhad Soleimanian Gharehchopogh " Mobile Cloud Computing: Security Challenges for Threats Reduction International Journal of Scientific & Engineering Research," Volume 4, Issue 3, March-2013 ISSN 2229-5518.

[9] Vahid Ashktorab2, Seyed Reza Taghizadeh1 "Security Threats and Countermeasures in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[10] Mr. D. Kishore Kumar "Cloud Computing: An Analysis of Its Challenges & Security Issues," International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012 www.ijcsn.org ISSN 2277-5420.

[11] K.S.Suresh " Security Issues and Security Algorithms in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering.

[12] Dr.A.Padmapriya M.C.A., M.Phil., Ph.DP.Subhasri, (M.Phil, Research Scholar)

"Cloud Computing: Security Challenges & Encryption Practices," Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[13]Leena Khanna " Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them," Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[14] F.A.Alvi, B.S.Choudary, and N.Jaferry, "Review on cloud computing security issues & challenges," iaesjournal.com, vol .2

http://searchcloudcomputing.techtarget.com/definition /private-loud .

[19] Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI,
"Homomorphic Encryption Applied to the Cloud Computing

Er. Ramandeep Kaur, *IJECS Volume 4 Issue 3 March, 2015 Page No.11045-11049*

(2012).

[15] Mandeep Kaur and Manish Mahajan, "using encryption algorithms to enhance the data security in cloud computing," International journal of communication and computer technologies, ISSN Number: 2278-9723.

[16] Gartner: Seven cloud-computing security risks InfoWorld 2008-07-02.

[17] Furht,B. and Escalante,A. (2010). Handbook of Cloud Computing. New York: Springer

Security," Proceedings of the World Congress on Engineering, Vol.1, WCE 2012, July 4 (2012), London, U.K .

[20]http://www.mytestbox.com/miscellaneous/cloud-computing-grid-computing-utility- computing-list-top-providers/