**International Journal of Cloud Computing and Services Science (IJ-CLOSER)**
Vol.3, No.5, October 2014, pp. 271~282
ISSN: 2089-3337

# Secure-Video Communication over Cloud

**Dinesh Goyal*, Naveen Hemrajani****
*Research Scholar, Suresh Gyan Vihar University, Jaipur, dinesh8dg@gmail.com
**Professor, JECRC University, Jaipur, naven_h@yahoo.com

**Article Info**

***Article history:***

Received Aug 30th, 2014
Revised Sept 25th, 2014
Accepted Oct 10th, 2014

***Keyword:***

Security
Cloud
Video
Encryption
Watermarking

**ABSTRACT**

The work proposed, & analyzed in this paper is focused on the development of secure video and its communication as a service for Video on Demand for Cloud environment. It targets many issues of security of video contents such is its accessibility (confidentiality) or validation (authenticity) during the communication over a network. It also attempts to optimize the cost (time) of multimedia security, which has three levels security, Access Control, Confidentiality & Authenticity. The work does not end with security of data but it also ensures fast delivery of the same to client using compression Techniques. These all have been deployed using different fast and reliable methodologies. Then these all are integrated on a Cloud Environment with secure network architecture. This gives user a fast and secure access to Video on Demand on a Public Cloud Environment.

***Corresponding Author:***

Dinesh Goyal
Departement of Computer Science & Engineering,
Suresh Gyan Vihar University
Mahal, Jagatpura, Jaipur, India, 302001
Email: dgoyal@gyanvihar.org

## 1. INTRODUCTION

Cloud Computing has been used to download resources required in computing capabilities, storage and security devices in the cloud and it has expended in technological arena leaps & bounds. It is expected that applications using internet video such as Video on Demand to be deployed and supported on the cloud to users should provide fast and good quality video service. However, providing video on demand to the cloud users over any networks presents many challenges. The security of video in this demanding environment remains an open research topic, and this in turn affects the visual quality of level of application and prevents the perceived quality of user experience (QoE).

In this work, one particular issue we focus on is the effect of security applications on the quality of streaming video service through the cloud. We design and implement a platform consisting of a Interface for users over wired or wireless network, in which our concept of computing, & secure video streaming are implemented and integrated to allow testing of our framework.. Geographical independence Mobility support is introduced to allow continuous streaming experience for a non-local user through the web portal.

## 2. CLOUD COMPUTING

"Cloud" is a term used for a virtual collection of computing resources. A wide range of benefits to consumers are offered the use of cloud computing: the availability of a huge variety of software applications, storage, seemingly limitless access to the processing power of lightning and the ability to share information easily worldwide. A user can access all of these benefits through your browser at any time once you have access to the Internet. In early 1990, a large ATM network became known as "the cloud" [6]**]**. The term appeared again, about twelve years ago with the advent of web services based on Amazon. Cloud computing allows consumers and corporate structures used by all applications that offers the cloud without the extra effort of installation and also offers access to your personal files from any computer with Internet access.

Cloud computing is intended to make the concept of computing as a utility, like water, gas, electricity and telephone. Also embodies the desire of the real services and computing resources. Software and informatics and computing infrastructure platform can all be considered as services with no concern as to how or from where they are actually render. The potential of cloud computing has been recognized by major industry players so that the top five software companies by sales volume, all have great deals cloud [1].

## 3. Video on Demand In cloud

Video-on-demand (VoD) has become a popular service on the Internet. Usually ISP provider billed today VOD for the use of bandwidth by 95 percentile rule, Since the demand of the users of a service VOD varies over time within a day, provisioning servers separate property for the 95 percentile value however, they must hold a couple of hours per day leads to underutilization of bandwidth at other times. For example, in PPLive [3], the duty cycle is less than 20% for more than 50% times with an average of 40%. The 95th percentile value is 5 times the lowest value. Moreover, the provision for a multitude of flash is extremely expensive, even if the flash mob can be predicted.

The self-owned servers, and owned providers of VoD, store all the original video files, used part of user requests and upload videos to the cloud storage. This shops cloud storage of video files and push these videos to your CDN cloud. Cloud CDN offers streaming content using a global network of edge locations [5].

From a site of large-scale VoD can store hundreds of thousands of videos and a large volume of traffic heading to the cloud solution VoD, requires that the cloud must store a huge amount of files to serve this type of traffic. While spending to upload these files is high, including the cost of cloud storage and especially the cost of bandwidth to upload the video to the cloud, we must carefully design our migration strategy. Obviously, the goal of designing a good migration strategy is to save the added cost, while minimizing user requests not satisfied as much as possible. In order to save the cost of cloud storage and the cost of renovation, we chose to store the most popular videos.

Meanwhile, [4] proposed VoDaaS and then analysed the performance of her model of Video on Demand as a Service (VoDaaS) based on the following criteria:

- The upload time and download time of the video files of varying sizes are divided into block blobs.
- The average upload and download time for a chunk of different block blob size of different video files.
- The throughput for both uploading and downloading of video files of varying sizes to the cloud storage.

### 3.1 Security of Video in cloud

Current Multimedia systems (digital communications) will make continuous media stream. It is very essential to stop the Hackers and eavesdroppers technically called as potential threats from corrupting or stealing the valuable information that is being passed through the Communication. Due to the demand for the streaming videos the applications for the streaming are going to be endless.

Main Aim of Secured Video transmission is to provide: authentication, content tracking, conditional access, copy control, confidentiality. The level of Security differs from each and every Video application. The application that needed security can be classified as: Entertainment applications like VoD and pay TV.

Personalized applications of video are like Business meetings, telemedicine, and diplomat dialogues etc. Though both the categories of applications need security, applications on Entertainment need low security when compared to the Video services that are personalized. Applications related to entertainment need to provide the video with more quality and timeliness. The Price of a High quality video is more when compared to that of the low quality videos, which makes the user to go for the high quality version of the video. For all the entertainment video applications verification of the User identities is must, where as in personalized applications digital signs and certifications are used instead [2]

Providing security for many Multimedia applications like Video on-Demand service, broadcasting a video, video-conferencing and multimedia mails is must. A secured video transmission ensures the user such that no unapproved eavesdroppers can get the information from the video while it’s being sent to receiver i.e. the users those who paid for these services can only watch the videos and movies. If the video is more redundant it helps the attacker to easily rebuild the original video file. Data such as text and program code has less redundancy when compared to videos in its structure. All these factors make providing security for a MPEG video more challenging. Providing security for these MPEG video transmission involves in encrypting parts of the MPEG bit stream or the entire bit stream.

Applying cryptography algorithms such as Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES) is one of the ways for providing security to multimedia applications, though they involve in complex computations. When one consider the whole data one can perform a heavy weight encryption algorithm which increases the problem and also latency. Whereas a light weight algorithm that provide enough security and also have a reasonable computation price for MPEG applications are used for encrypting the selective or partial data. In [2] presented the most effective algorithm for MPEG video encryption which is based on AES encryption algorithm which is a light-weight encryption algorithm that uses selective encryption method. This algorithm is based on a light-weight selective encryption algorithm RVEA which was based on DES and IDEA. By Adopting the AES algorithm to encrypt the data security had increased significantly. This Algorithm also reduced the computational time by reducing the maximum size of the bits selected. Streaming can actually be done as a complete video package of a linear programming, as a subscription package (monthly pay), or as a pay per view service (pay based on data streamed). It might be as a part of a website or it is a tool for video preview and film dailies. Some applications are Internet broadcasting (corporate communications) education (viewing lectures and distance learning), web based channels (IP-TV, Internet radio), Video-on-demand (VOD) and Internet and intranet browsing of content (asset management). Such systems use different types of encryption techniques to increase the security precautions for networked multimedia applications.

## 4. PROPOSED WORK

Here we propose the integrated model of all the Video security, Authentication & Compression technique for Video-on Demand service over cloud. In our work, a Cloud environment is developed, to provide Video on Demand as service and name it as “Secure Video Communication over Cloud (SVCOC)”.

### 4.1 Cloud Deployment

The cloud deployment of SVCOC was done using VMware tools and XAMPP stack. On each physical server VMware ESXi hypervisor is installed. Then a management Windows server was deployed with VMware vCenter Server over it. The vCenter server monitors all the ESXi servers and creates a cluster out of them, with each physical server acting as a node. A Windows Server 2012 R2 virtual machine is then deployed on the cluster which is set to operate for maximum efficiency. The virtual machine is then used as the base for the Apache, MySQL, PHP stack (XAMPP). The MATLAB Software is also installed on the virtual machine, which would be used to run all the scripts of video communication, watermarking, encryption & compression. The XAMPP stack behaves as an interface between the MATLAB and PHP script running on the cloud side. The Cloud deployment is done over multi core servers. Which has above said software’s installed for the Cloud & Video on Demand Service. The client side PHP script invokes the Video Service requested by the user and communicates the same to the XAMPP stack which invokes MATLAB to provide the secure service to the user through PHP.

### 4.1.1 VMware ESXi

VMware ESX and VMware ESXi are Type 1 hypervisors that are VMware's enterprise software hypervisors for guest virtual servers that run directly on host server hardware without requiring an additional underlying operating system.

The host server requires some form of persistent storage (typically an array of hard disk drives) that stores the hypervisor and support files. A smaller footprint variant, ESXi, does away with the first requirement by permitting placement of the hypervisor on a dedicated compact storage device. Both variants support the services offered by VMware Infrastructure.

### 4.1.2 VMware vCenter Server

VCenter Server is installed at the primary server of a virtualized data center and operates as the virtualization or virtual machine manager for that environment. It also provides data center administrators and a central management console to manage all the system's virtual machines.

Virtual center provides statistical information about the resource use of each virtual machine and provisions the ability to scale and adjust the compute, memory, storage and other resource management functions from a central application. It manages the performance of each virtual machine against specified benchmarks, and optimizes resources wherever required to provide consistent efficiency throughout the networked virtual architecture. Besides routine management, virtual center also ensures security by defining and monitoring access control to and from the virtual machines, migration of live machines, and interoperability and integration among other Web services and virtual environments.

### 4.1.3 Windows Server 2012 R2

Windows Server is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications. Previous versions of Windows Server have focused on stability, security, networking, and various improvements to the file system. Other improvements also have included improvements to deployment technologies, as well as increased hardware support. Microsoft has also created specialized SKUs of Windows Server that focus on the home and small business markets. Windows Server 2012 R2 is the latest release of Windows Server, and focuses on cloud computing. Windows Server works for providing platform to deploy the applications for the client side applications.

### 4.1.4 XAMPP (Apache, MySQL, PHP) Stack

XAMPP stands for “X (as in “cross-platform”), Apache, MySQL, PHP, and Perl” and is an “AMP stack package” that installs each of these software’s. An AMP’s fancy way of saying is “bunch of Apache, MySQL and PHP for web Development”. The package helps in easier deployment of web servers. XAMPP allows you to run a web server that will interpret web sites that run on PHP, Perl, or HTML

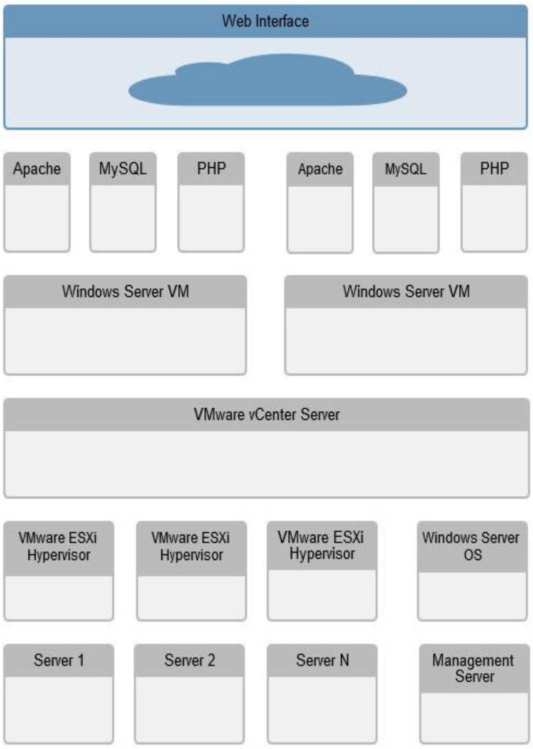

Figure 1. Stack Diagram of Diagram of Video on Demand Service over Cloud

### 4.2 Workflow Description of the SVCOC

As described earlier “Secure Video Communication over Cloud” is a cloud based service which focused on provides a secure video communication to user. The “SVCOC” enables the client to access the service anytime anywhere. SVCOC is a video manager which will manage the videos uploaded by users. The videos can be free or paid, SVCOC will encrypt both types of video while uploading. To upload a video user will need to provide video details and a watermark.

When a client try to access the services of SVCOC it prompt user to input login details to continue. When user will submit the credentials the SVCOC will cross check the user’s database using MySQL and PHP, if the entry found, user will be proceeded to user’s uploads else it will show login error.If user is not registered with SVCOC, he will need to register with SVCOC. After successful registration and login, user will be able to see his uploads. After login there are three tabs:

1. My Uploads: This tab consists of all uploads of logged in user.
2. Free Videos: This tab consists of all free videos which are uploaded to SVCOC.
3. Paid Videos: This tab consists of all paid videos which are uploaded to SVCOC.

As depicted in below given flow chart, to upload any video, user will need to go in “My Uploads” tab. User will need to provide few details and a watermark. The video will be uploaded & encrypted on the server. A progress bar will be visible during the whole process. To download any video, user will need to click any video under a particular tab. User will get two links after decryption of video, one is for stream the video on his panel and other one is for download video to his hard drive. If the video is uploaded by him, he will also get the link to download the extracted watermark. If user wants to download Paid Videos, he will be required to pay the video price then only the video will be decrypted and available for download to him. The download facility is available only for public video for any user. Private videos whether paid or free are not accessible by users except the owner of the video, who has uploaded the same.

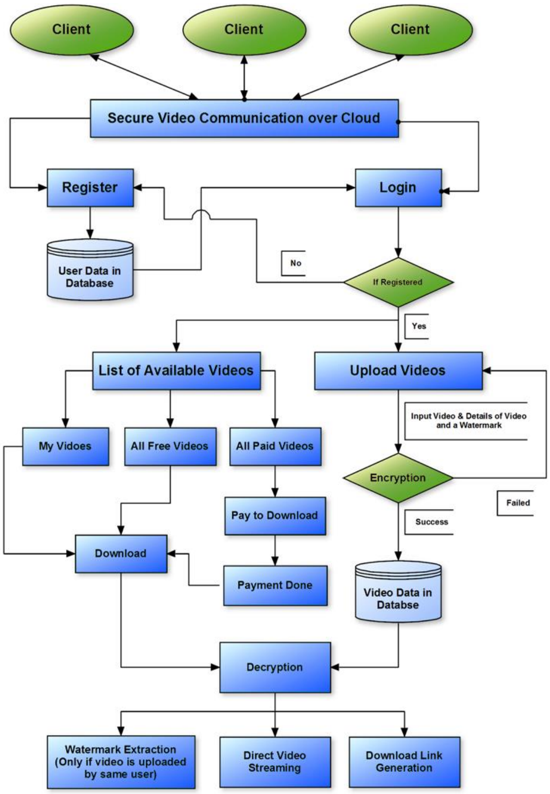

Figure 2. Work flow diagram of the Video Manager

After doing all the design and deployment of Video service and security over cloud, now we analyze the performance of video uploading & Downloading. We will do this analysis with a specific video whose snapshots are as follows:

Figure 3. Snapshots of Test Video

This video is having frame size of 400*224 and has been converted in 4 formats namely AVI, WMV, MPEG, H.264 (MP4). Then these four types of video has been further cropped in length to have 4 sizes of video namely 256KB, 512 KB, 1024KB and 2048 KB each.

This composite data set helps us to analyze performance of the Video formats over our cloud environment and quantifies the range of services rendered by SVCOC. The analysis can be divided into two major components.

- Performance of Individual Video Formats on Varying sizes
- Performance of Same size videos with different Video formats.

We first start with performance analysis of Individual video formats for all four types of video formats. The data in Table 1 shows the time taken for uploading & downloading of each and every video (including watermarking, encryption and compression).

Table 1. Video types & size and their performance

| Size & Type of Video in KB | Upload Time(sec) | Download Time (Sec) |
|---|---|---|
| AVI 256 | 72.823 | 47.256 |
| AVI512 | 136.682 | 84.434 |
| AVI 1024 | 160.584 | 95.547 |
| AVI 2048 | 500.673 | 308.157 |
| WMV 256 | 63.862 | 57.156 |
| WMV 512 | 105.652 | 69.822 |
| WMV 1024 | 186.841 | 125.451 |
| WMV 2048 | 296.399 | 247.322 |
| MPEG 256 | 95.732 | 37.227 |
| MPEG 512 | 166.966 | 49.819 |
| MPEG 1024 | 179.204 | 89.886 |
| MPEG 2048 | 582.276 | 158.6678 |
| H.264 256 | 51.661 | 41.671 |
| H.264 512 | 90.888 | 47.696 |
| H.264 1024 | 172.767 | 98.011 |
| H.264 2048 | 290.761 | 184.173 |

**AVI Video: Uploading Times**

The growth in timing is almost consistent for AVI Video as shown in Figure 4

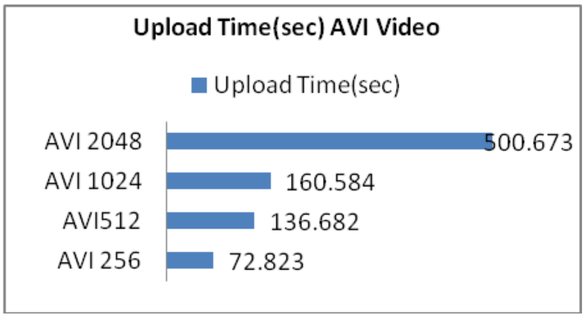

Figure 4. AVI Video Upload Timing

**AVI Video: Downloading Times**

The growth in timing is almost consistent for AVI Video as shown in Figure 5 but there is marginal extra growth in time to upload a 2MB Video.

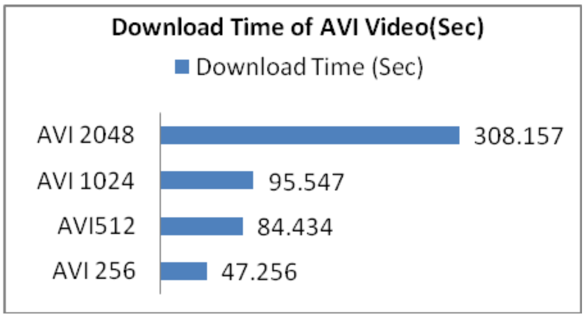

Figure 5. AVI Video Download Timing

### WMV Video: Uploading Times

The growth in timing is almost consistent for AVI Video as shown in Figure 6 but the time taken to upload the video is comparatively very high.

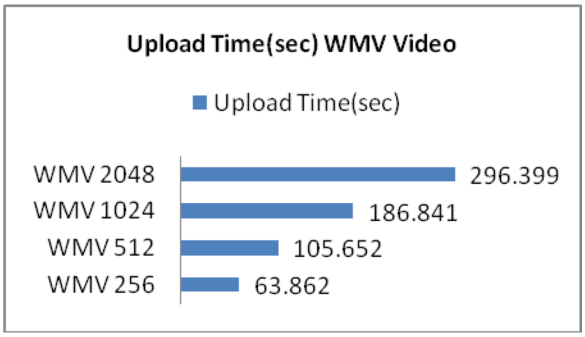

Figure 6. WMV Video Upload Timing

### WMV Video: Downloading Times

The growth in timing is almost consistent for WMV Video as shown in Figure 7 but the time taken to download the same is not so high.

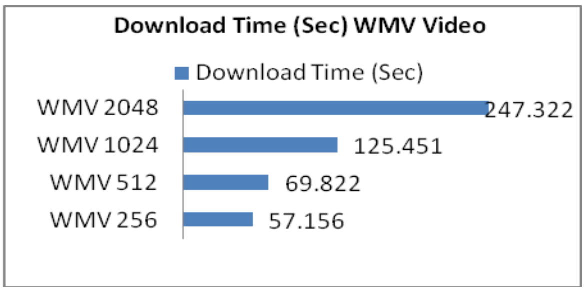

Figure 7. WMV Video Download Timing

### MPEG Video: Uploading Times

The growth in timing is almost not at all consistent for MPEG Video as shown in Figure 8, also there is marginal growth in time to upload all the videos.

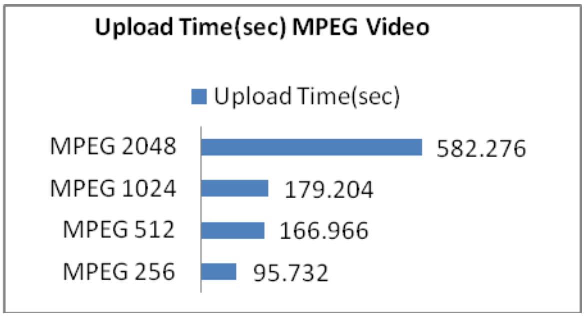

Figure 8. MPEG Video Upload Timing

### MPEG Video: Downloading Times

The growth in timing is almost consistent for MPEG Video as shown in Figure 9

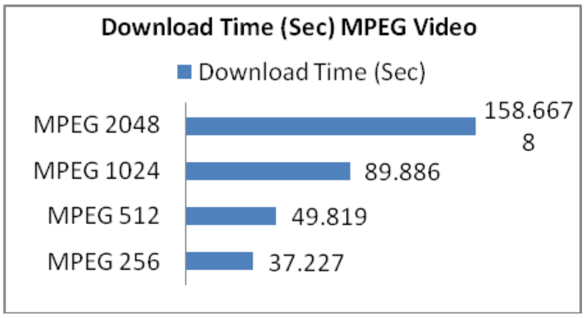

Figure 9. MPEG Video Download Timing

**H.264 Video: Uploading Times**
The growth in timing is very much consistent for H.264 Video as shown in Figure 10 and the timing are optimal for the upload process.

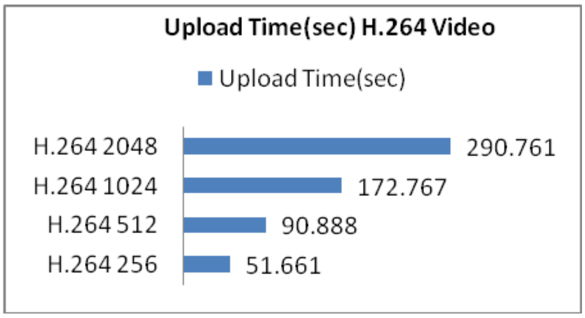

Figure 10. H.264 Video Upload Timing

**H.264 Video: downloading Times**
The growth in timing is very much consistent for H.264 Video as shown in Figure 11 and the timing are optimal for the download process too.

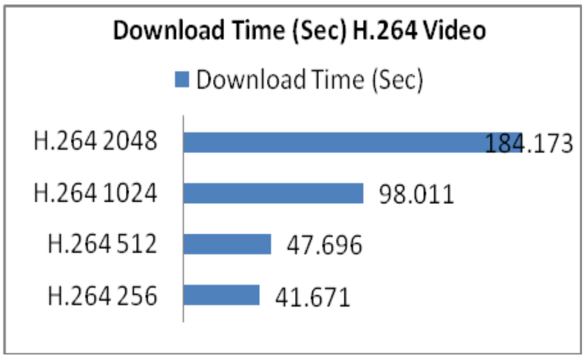

Figure 11. H.264 Video Download Timing

Now let us analyze the performance comparatively of same size of different types.

**256 KB Video: uploading Times**
For 256 KB the H.264 video takes minimum time to upload the video over SVCOC as depicted in Figure 12

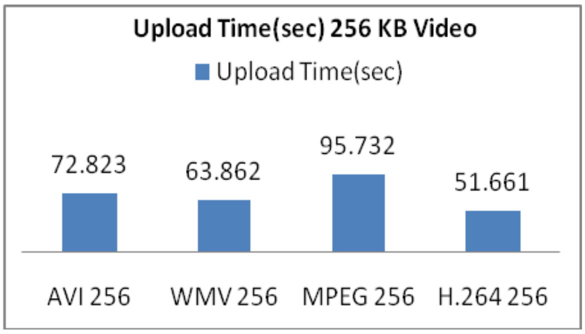

Figure 12. 256 KB Video Upload Timing

**512 KB Video: uploading Times**
For 512 KB the H.264 video takes minimum time to upload the video over SVCOC as depicted in Figure 13

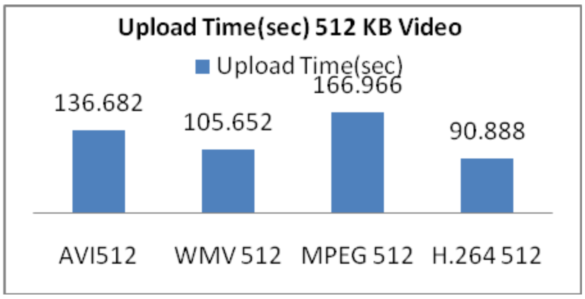

Figure 13. 512KB Video Upload Timing

**1024 KB Video: uploading Times**
For 1024 KB the AVI video takes minimum time to upload the video over SVCOC as depicted in Figure 14.

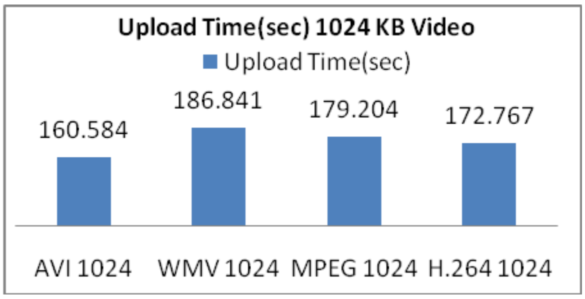

Figure14. 1024 Video Upload Timing

**2048 KB Video: uploading Times**
For 2048 KB the H.264 video takes minimum time to upload the video over SVCOC as depicted in Figure 15

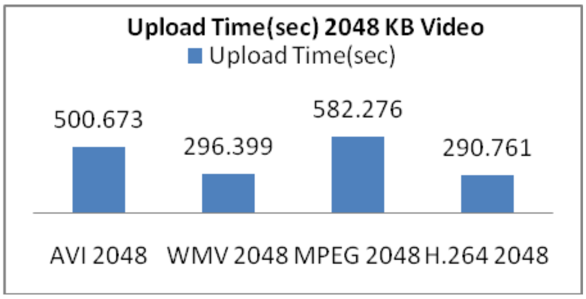

Figure 15. 2048 KB Video Upload Timing

**256 KB Video: downloading Times**
For 256 KB the MPEG video takes minimum time to download the video over SVCOC as depicted in Figure 16

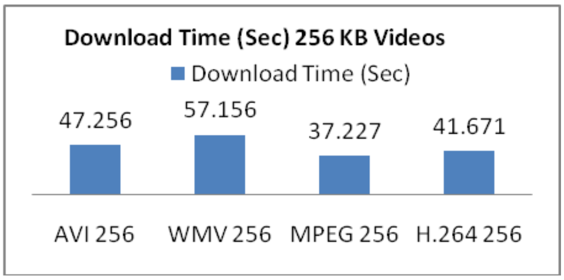

Figure 16. 256 KB Video Download Timing

**512 KB Video: downloading Times**
For 512 KB, H.264 video takes minimum time to download the video over SVCOC as depicted in Figure 17

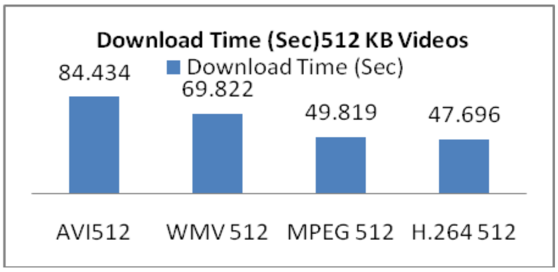

Figure 17. 512 KB Video Download Timing

**1024 KB Video: downloading Times**
For 1024 KB the MPEG video takes minimum time to download the video over SVCOC as depicted in Figure 18

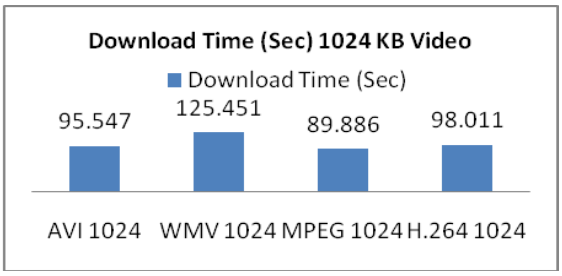

Figure18. 1024 KB Video Download Timing

**2048 KB Video: downloading Times**
For 2048 KB the MPEG video takes minimum time to download the video over SVCOC as depicted in Figure 19

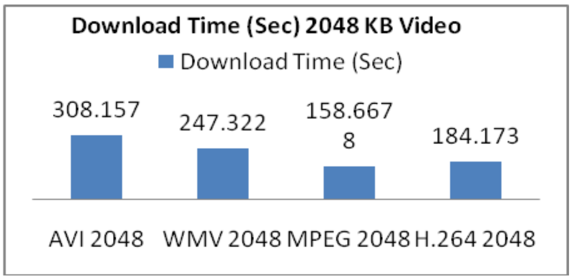

Figure 19. 2048 KB Video Download Timing

## 5. CONCLUSION

Today the cloud environment has become more popular day by day and they are now in reach to the people who are not even aware about definition of cloud. Yet the Cloud environment is facing the issue of Vulnerability as they are less secure. In order to resolve the issue, here we have proposed, designed and deployed the integrated model of all the proposed Video security, Authentication & Compression technique for Video-on Demand service over cloud. In our work, a Cloud environment is developed, to provide Video on Demand as service. For the same we have created a Cloud environment with Multi core processor based machine with 8 GB RAM with Windows 2012 Server R2. Server was deployed with hypervisor and PXE & RDP server. The PXE Servers works for Network Management, while RDP Server helps access of Cloud for the end user, it can be accessed by using with hypervisor using VMWare. Then the MATLAB & XAMPP server is deployed over the VMWare for Video on Demand Service. The XAMPP behaves as interface between the client and the MATLAB for encryption/decryption or watermarking/de-watermarking. This whole deployed is done without any codec and still the results are very good without block wise execution of security process.

The Video manager portal designed for the end user gives the user a facility to maintain his video library online, he can even share videos for other users or can keep them private for himself only. Both the proposed security techniques have been integrated into the Cloud environment for the security of content uploaded by the user. The user who has uploaded his video can download the video and get his watermark back too. While any other user who accesses the same video if public can only get the video but cannot access the watermark of the video. Then an analysis has been performed to get the feel of how the environment serves the end user for various kind of video formats and how it is better than existing techniques of security when deployed with our proposed cloud environment. Our analysis of comparison of various video formats over the SVCOC gives that compressed video namely MPEG and H.264, perform better in terms of uploading and downloading the video, whilst uncompressed Video like AVI take lot of time for encryption, watermarking and uploading. While downloading also the MPEG and H.264 are far-far better than that of other formats and good for end users and they are fast to access and have better video quality too.

### 5.1 Future work

At the end we may suggest research to develop a cloud environment for enhancing the results obtained by us and give more users friendly and secure video communication over cloud. Even researchers can design protocols like SSL using these security techniques for real time streaming services too.

## References

[1] Chow et. al. 2009, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”. In Proceedings of ACM workshop on Cloud computing security

[2] Govinda et. al., 2013, “On-Demand Secure Streaming of Multimedia Data over Cloud”, International Journal of Engineering and Technology, Vol. 5 No 3, Page No. 2101-2107

[3] Huang et. Al., 2008, “Challenges, Design and Analysis of a Large-scale P2P-VoD System” In Proc. of ACM SIGCOMM

[4] Lavanya et. al., 2011, “Cloud Based Video on Demand Model With Performance enhancement”, Malaysian Journal of Computer Science, Vol. 24 No. 2, Page No. 73-83

[5] Li et. al., 2011 “Cost-effective Partial Migration of VoD Services to Content Clouds”, IEEE 4th International Conference on Cloud Computing, 978-0-7695-4460-1/11 Page No. 203-210

[6] Maggiani, 2009, “Cloud Computing Is Changing How We Communicate”, In IEEE 978-1-4244-4358-1/09

[7] Cha et. al., 2012, “Design of StraaS (Streaming as a Service) based on Cloud Computing” International Journal of Multimedia and Ubiquitous Engineering, Vol. 7, No. 4, Page No.187-200

[8] Gaeta et al., 2013, “StreamSmart: P2P Video Streaming for Smartphones Through The Cloud”, Vol. 60. In SECON

[9] Guleria et. al., 2013, “To Enhance Multimedia Security In Cloud Computing Environment Using Crossbreed Algorithm” International Journal Of Application or Innovation in Engineering & Management , Vol. 2, No 6, Page No. 562-568

[10] Huang, et. al. 2011, "CloudStream: Delivering High-Quality Streaming Videos through a Cloud-Based SVC Proxy," in IEEE INFOCOM Mini-Conference

[11] Nithyabharathi et. al., 2014, “To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES”, International Journal of Science, Engineering and Technology Research, Vol. 3, No. 2, Page No. 341-34

## BIOGRAPHY OF AUTHORS

**Dinesh Goyal.** Research Scholar, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur, India. In his 14 years of research and academic experience, has published more than 40 International & National papers in the area of , Image Processing, Information Security, Cloud Computing.

**Dr. Naveen Hemrajani.** HOD & Professor, Department of Computer Science & Engineering JECRC University, Jaipur, India. In his more than 20 years of research and academic experience, he has published more than 50 International paper on the field of Information & Network Security, Software Engineering. He has also guided more than 5 Ph.D. research scholars and 30 M.Tech Students.