ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (43-46), Month: April - June 2016, Available at: www.researchpublish.com

MOViEDuS: Multipart Offline Video Encryption and Distribution System

Ashin Mathew[1], Vishnu Gupthan[2], Sneha Thankachn[3]

[1,2,3] MG University, Mar Baselios Christian College of Engineering and Technology, Peermade, Kerala, India

Abstract: **Piracy in video distribution is a challenging problem nowadays. There are many studies and researches done to prevent the piracy. We can find some of the main reason for increased piracy is unavailability of the video to the user, increased cost of video. The low bandwidth of internet makes the users to download the video to view them without interruption. The downloaded video is distributed using Bluetooth, hotspot sharing, flash drives, optical disks etc. The proposed systems solve this problem by splitting the video content and encrypting each part. To view the video content a ticket is needed. The users have to pay for the ticket. The video content can be shared among users without violating copyright laws.**

Keywords: **Video Encryption, Distribution, Piracy, Compression, Video Splitting.**

I. INTRODUCTION

The video streaming is an important field of research today. The main problem we are facing in video streaming is low bandwidth [1]. Many solutions have been discovered to solve this problem. It is not possible to stream a video if the bandwidth is too low. Many places in the world does not have high speed internet connectivity. This problems make the users to download these videos. This will violate the copyright laws. We cannot stream video because of the low bandwidth of the internet and we cannot allow the users to download the videos because it will violate copyright laws.

Nowadays there are many ways to distribute a file. This will create a mass distribution of video files. These methods are not monitored by any authority thus making them impossible to track. The only way to prevent it is to stop at the source. The distribution of a copyright protected video is like a virus outbreak. The only way to completely stop the illegal distribution is to stop the first malicious user or patient zero. But it is not always possible to find the patient zero. So we need to prevent the video from reaching the malicious user, it is not practically possible.

In this paper we propose Multipart Offline Video Encryption and Distribution System MOViEDuS. MOViEDuS allows the user to download videos without copyright violation. The content provider distribute the video to the users. The patient zero is not able to distribute the video illegally. MOViEDuS allows the user to share the video but the next user is not able to view the video without the permission of the content provider.

The MOViEDuS has two main phases. Phase 1, the encryption phase split the video file into multiple parts and encrypt each part. The encrypted video files are compressed into a zip file. The zip file contains the entire video file. This zip file is made available for all users. Phase 2, viewing phase unzip the encrypted file and decrypt them using a ticket. The user does not get the actual decryption key so the user cannot decrypt the file himself.

II. RELATED STUDIES

The network friendly video distribution [2] which is a method to avoid network bottleneck due to large demand for video streaming services. This method guaranties improve delivered Quality of Service (QoS). This method efficiently deploy an Information Centric Networking (ICN) architecture.

Flash crowd avoidance in P2P video on demand streaming via pre-release distribution [3] is a method to avoid sudden increase of demand for a video especially during its release time. This method allows pre-release video distribution. The users are allowed to download an encrypted version of a video before the release of the video. During the time of video release the decryption key for the video is given to the users. The users can use this key to decrypt the video and watch it

Video encryption for secure multimedia transmission layered approach[4] uses a timer selective video encryption methodology this methodology use a concept of row/column permutation, effectively shuffles the video data resulting in faster and better encryption of video data. The video stream is quite different from traditional textual data.

Modified AES based algorithm for MPEG video encryption [5] uses an advanced encryption standard algorithm to reduce the calculation of the algorithm and for improving the encryption performance. Turbocharged Video Distribution via P2P [6] uses a mesh-based video distribution system without depending on video replication on streaming peers.

WiVision [7] uses IEEE 802.11 wireless LANs as the last mile for both real-time video distribution and on-demand video playback. WiVision can air both live events, such as on-campus seminars and sports activities, and pre-stored video streams, such as course lectures and financial analysis sessions, to mobile users, who can tune in to selected channels of their choice from their laptops.

III. MOViEDuS: MULTIPART OFFLINE VIDEO ENCRYPTION AND DISTRIBUTION SYSTEM

The MOViEDuS is an advanced video distribution method which ensures copyright protection in videos. MOViEDuS uses encrypted video files which makes the user impossible to view without the permission of the owner. MOViEDuS split the video and encrypt it so in order to recover the original content all the encrypted slit files have to be decrypted. The MOViEDuS does not provide the actual decryption key to the user. So the user cannot decrypt the file. Instead of actual decryption key a ticket is issued to watch the content. In order to get a ticket the user has to pay the owner of the video content. The MOViEDuS video player accept the ticket and authenticate the ticket with the MOViEDuS server. If the ticket is authenticated the decryption key is sent to the MOViEDuS video player by the MOViEDuS server and the player decrypt the video and plays it. The content provider can choose any key for encryption during the encryption phase and the user is never aware of the key.

A. Encryption phase:

In the encryption phase the video file is split into a fixed number of small pieces. All the pieces have the same size. The size of a piece can be found out by dividing the actual video file size by the number of pieces.

$$Sizeof(i^{th}piece) = \frac{sizeof(video\ file)}{N}$$

Where N is the number of pieces. The value of N should be equal for all the video files. This value cannot be changed once the MOViEDuS is implemented. Each video file is encrypted using DES encryption algorithm. The encrypted video files are compressed into a zip file. The zip file contains the entire video content as multiple encrypted video files. The content provider can upload the zip file and the decryption key to the MOViEDuS server.

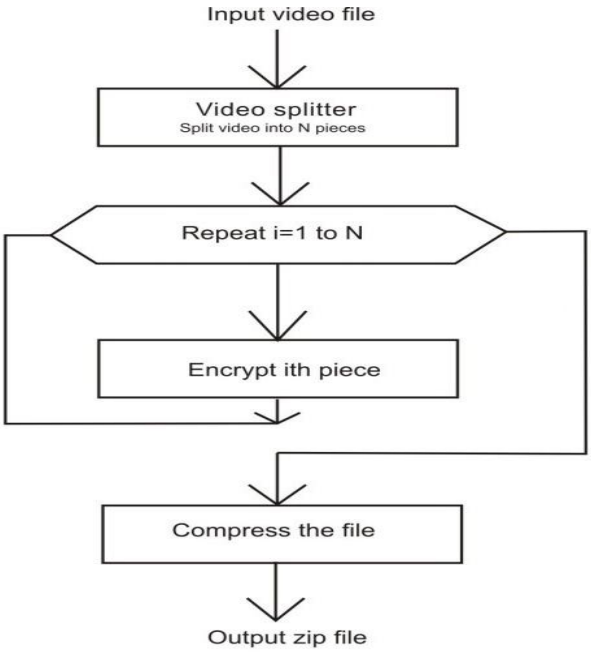

Fig 1. Flowchart of encryption phase

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (43-46), Month: April - June 2016, Available at: www.researchpublish.com

B. MOViEDuS Server:

MOViEDuS server contains all the video content as a zip file. The zip files are created during the encryption phase. The server also contains the decryption key associated with each zip file, the details of all the content providers and the users who are registered with MOViEDuS. The users can download the zip file containing the encrypted video file from the server any time.

Once a user downloads the file from the MOViEDuS server other users do not have to download the file again. The zip file can be transferred from one user to another user using any file transfer mechanism. Thus a user with a slow internet connection does not have to wait hours to download the file. Once a user has the zip file, the user can login to his account in MOViEDuS and buy the ticket for that file. The user has to pay the amount put by the content provider.

C. Viewing phase:

The viewing phase consist of the MOViEDuS video player. The MOViEDuS video player is the most important part in the MOViEDuS. The video player plays the video files sequentially. The player asks the user to select the zip file containing the encrypted pieces and to enter the ticket. The player authenticate the ticket and zip file user selected. The player check whether the entered ticket zip pair has a match in the server. If the match is found the decryption key is sent to the player. The player decrypt and play the files sequentially. After playing each piece the decrypted file is deleted and next piece is encrypted. The player does not allow the user to pause the video so the user cannot reassemble the decrypted pieces as they are playing.

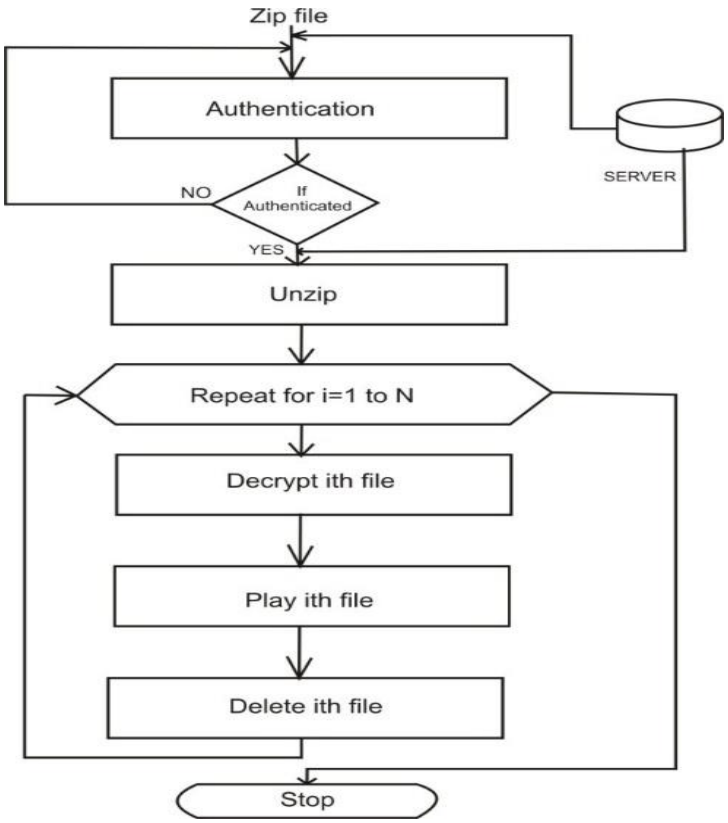

Fig 1. Flowchart of viewing phase

IV. ADVANTAGES

The MOViEDuS has many advantages over existing systems. The MOViEDuS ensures copyright protection. The files in the MOViEDuS cannot be used illegally. Also once a file is downloaded by a user, another user may not need to download the same file. The users can copy the file from one user to another user. Since the files are encrypted there is copyright protection. A user with a slow internet connectivity or a metered internet connection can download the file from another connection or can copy it from a user who already has the file.

The MOViEDuS allows the content provider to set a reasonable price for the content, so the user can also buy the ticket at a reasonable price. The MOViEDuS can provide High definition and standard definition videos. The user can buy as many tickets as the user needs by paying the amount. Once a ticket is bought it is possible that a malicious user can share the key. The MOViEDuS will allow a key only a limited number of time based on the amount paid, so the key is valid only for a number of times. The actual decryption key is not available to the user. The decryption key is only known to the content provider and MOViEDuS server. The MOViEDuS can be used to distribute new video contents through internet where the provider is not able to distribute using traditional methods

V. CONCLUSION

The MOViEDuS ensure the protection of the video content against piracy. The MOViEDuS video content can be received from any user who has the video content. The decryption key is not available to any user only the ticket is given, so the user cannot view the actual video content without the ticket. To authenticate the ticket the user need an internet connection but a low bandwidth metered connection is enough for authentication. Once the ticket is authenticated there is no need for the internet connection. The MOViEDuS videos are similar to an ordinary video but in order to view the video a valid ticket is needed. Thus the MOViEDuS can be used to distribute videos by the content provider where traditional video distribution is not possible.

REFERENCES

[1] Riccardo Bernardini, Roberto Rinaldo, "Copyright Protection in Peer-to-Peer Networks for Video-on-Demand Streaming", IEEE International Conference on Communications 2013: IEEE ICC'13 - Workshop on Cloud Convergence: challenges for future infrastructures and services.

[2] Z. LiM, K. Sbaï , Y. Hadjadj-Aoul, A. Gravey, D. Alliez, J. Garnier , G. Madec, G. Simon, K. Singh, "Network friendly video distribution", 2012 Third International Conference on the Network of the Future (NOF).

[3] S. K. H. Chiu, S. T. Vuong, "A novel method for flash crowd avoidance in P2P video on demand streaming via pre-release distribution", 2008. ATC 2008. International Conference on Advanced Technologies for Communications.

[4] T. P. Pai, M. E. Raghu, K. C. Ravishankar,"Video Encryption for Secure Multimedia Transmission - A Layered Approach",2014 3rd International Conference on Eco-friendly Computing and Communication Systems (ICECCS)

[5] P. Deshmukh, V. Kolhe,"Modified AES based algorithm for MPEG video encryption",2014 International Conference on Information Communication and Embedded Systems (ICICES).

[6] Chunfeng Yang, Yipeng Zhou, Liang Chen, Tom Z. J. Fu, and Dah Ming Chiu, "Turbocharged Video Distribution via P2P",IEEE Transactions on Circuits and Systems for Video Technology Vol:25, No 2 pp.287-299 August 2014

[7] P. De, S. Sharma, A. Shuvalov, Tzi-cker Chiueh,"WiVision: a wireless video system for real-time distribution and on-demand playback ", 2004 1ST IEEE Consumer Communications and Networking Conference.