International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN: 2349-9745
p-ISSN: 2393-8161

Enhanced Dynamic Leakage Detection and Piracy Prevention in Content Delivery Networks

J.Joslin Iyda[1], R.ThangamalarAnitha[2]
[1]Information Technology, Rajalakshmi Engineering College
[2] Information Technology, Rajalakshmi Engineering College

Abstract -- Due to the increasing popularity of video services application in recent days, it is undesirable to prevent the content leakage on the trusted video delivery and piracy prevention has been indeed, become critical. In order to preserve content leakage and prevent piracy, conventional system addressed the issue by proposing the method based on the observation of streamed traffic throughout the network .Also piracy has hindered the use of open peer to peer networks for commercial content delivery. Hence the basic idea is to propose an enhanced dynamic content leakage detection scheme that is robust to the variation of the video lengths. It enhances the detection performances even in the environment subjected to variation in length of videos. To detect pirates, identity-based signature and time stamped token have been generated. It helps to solve piracy without affecting P2P clients so that colluder cannot download the secured videos. The advantage lies mainly in advanced content availability, low cost and copyright agreements in protecting the secured videos.

Keywords -- Content Delivery Networks, Content Leakage Detection, Streamed Traffic, Piracy, Digital Signature.

I. INTRODUCTION

In recent years, popularity of real-time video and streaming application and services over the internet has increased. Examples: YouTube, Microsoft Network Videos. Most people do not read as much as they used to, and when they do read, they tend to skim-read, which means the importance of written copy can be lost or misinterpreted[7].With an abundance of content pushed to consumers and employees every day, a well-crafted video allows brand or message to stand out and be clearly understood. The three basic reasons to use video: cost-effectiveness, increased productivity and consistency [8].

The main uses of videos [9] include Training and Tutorial, where corporate video first gained prominence with training (service, support, sales, personal development etc.) and continues to be one of the best uses of video. Online Video is a cost effective substitute for in-class training. It can also easily integrate video into online training management tools. Share the knowledge gained at these events by capturing the presentations, demos, interviews, commentaries etc. on video. Product Demonstrations help to show how product works and highlight the features that differentiate it from those other competitors. Software screen captures, 3D cut-away, or a high impact demo by a presenter are all excellent ways of showing how

e-ISSN: 2349-9745
p-ISSN: 2393-8161

product or service works. Infomercials have been around forever. While they continue to be the primary focus of web-based parody videos they have remained remarkably resilient over time. The shopping channel is, in effect, a 24 hour infomercial. If done well, Infomercials can be very effective at selling certain consumer products.

II. RELATED WORK

In computing, a shared resource, or network share, is a computer resource made available from one host to other hosts on a computer network. Some examples of shareable resources are computer programs, data, storage devices, and printers. Network sharing is made possible by inter-process communication over the network.

Shared resources, also known as network resources, refer to computer data, information, or hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise intranet. Successful shared resource access allows users to operate as if the shared resource were on their own computer. The most frequently used shared network environment objects are files, data, multimedia and hardware resources like printers, fax machines and scanners[10].

The videos with collusive piracy is the main source of intellectual property violations within the boundary of a P2P network. Paid clients may illegally share copyrighted content files with unpaid clients (pirates). Such online piracy has hindered the use of open P2P networks for commercial content delivery. It propose a proactive content poisoning scheme to stop colluders and pirates from alleged copyright infringements in P2P file sharing. The basic idea is to detect pirates timely with identity-based signatures and time stamped tokens. The scheme stops collusive piracy without hurting legitimate P2P clients by targeting poisoning on detected violators, exclusively[1].

Cisco Data Loss Prevention (DLP) is a data leakage protection solution that helps organizations assess risk and prevent data loss over the highest points of risk. It safeguards proprietary information against security threats due to enhanced employee mobility, new communication channels, and diverse services.

To solve the issues of content leakage, leakage detection scheme have been introduced. It helps to investigate the performance of the proposed method under a real network environment with videos of different lengths. The proposed method allows flexible and accurate streaming content leakage detection independent of the length of the streaming content, which enhances secured and trusted content delivery[2].

Video streaming application[3] deals with several P2P network is used to build live and online video streaming services on the internet at low cost. Provide large scale live and on-demand videos streaming services. The limitation is that no good quality of videos. Videos playback start tens of second after a user selects a channels.

e-ISSN: 2349-9745
p-ISSN: 2393-8161

In order to detect illegal content streaming by using traffic pattern which are constructed from the amount of traffic routers. To solve burst errors and random errors. It prevent content leakage from user‘s side. However delay occur due to large length of videos[4].

As an extensible signaling protocol, SIP (Session Initiation Protocol) can be applied in developing video conference system of conference server and the availability of bandwidth. It focuses on how to keep conferencing when the number of conference users increases. It provides a scalable service model for SIP-based video conference. The main disadvantage is Cost Expensive, Low resolution[5].

IPSec VPNs is developed to implement Internet security connection using Virtual Private Network. It helps in performing of video conference in real time multi-media traffic and secure connection links. Quality of video will be good. However due to heavy network, traffic loads. Encryption require high amount of CPU and memory [6].

Thus from the above it is concluded that content leakage and piracy prevention is a major issues. Hence it is proposed to recover content leakage and piracy for the trusted videos.

III. FRAMEWORK

In the framework, overall process of the design is being explained. The owner or distributor uploads the compressed video in the server. He uploads the copyright videos containing token, digital signature. Then the user is one who downloads the video. While he downloads the video, he needs to send request to server containing token, timestamp, signature .After the token and signature is being verified, the user can download that video in a compressed format. If the token or signature is not same, the videos can’t be downloaded. Thus the piracy of video is prevented.

When user uploads many videos in the server, content is being leaked due to the traffic of network. It can be identified based on the length of the video. Also when many users download the particular video, content is being leaked. So that the user can’t download the entire complete video. It should be avoided by leakage detection process. When leakage detection algorithm is being applied, content leakage is recovered. Thus the content leakage due to traffic of network can be avoided.

The overall architecture diagram for the content leakage and piracy prevention is given below.

The methodology of the proposed framework is based on the following module.

1. Video Compression

2. Piracy Prevention

3. Content Leakage Detection

4. Content Leakage Recovery

e-ISSN: 2349-9745
p-ISSN: 2393-8161

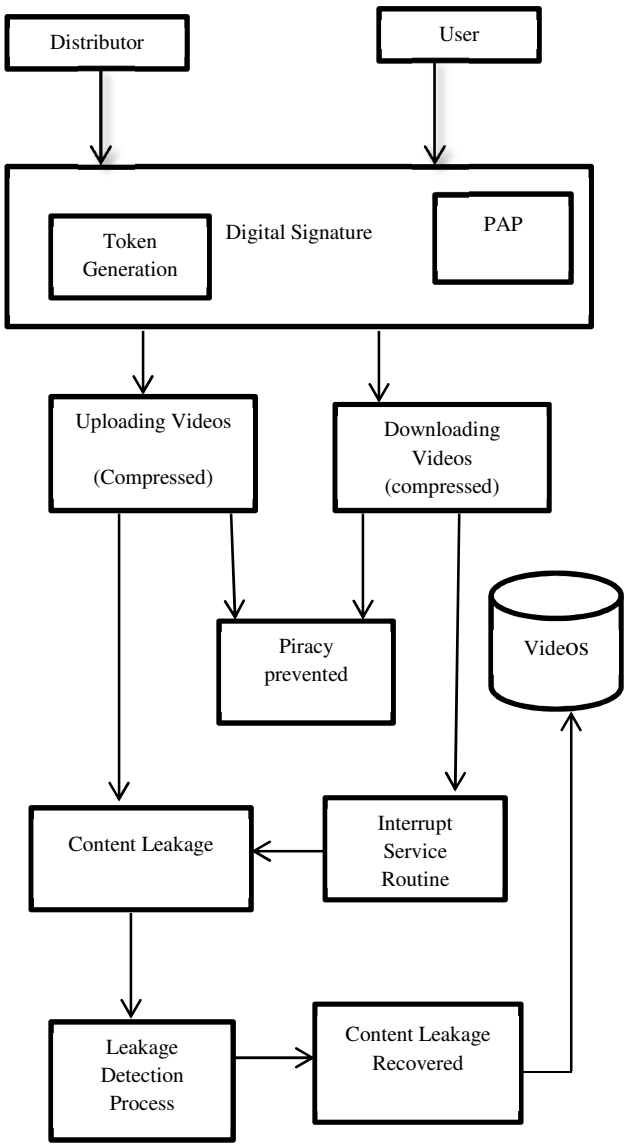

Figure 1. Framework for Content Leakage and Piracy Prevention

e-ISSN: 2349-9745
p-ISSN: 2393-8161

The Dataflow diagram for the overall framework is given below.

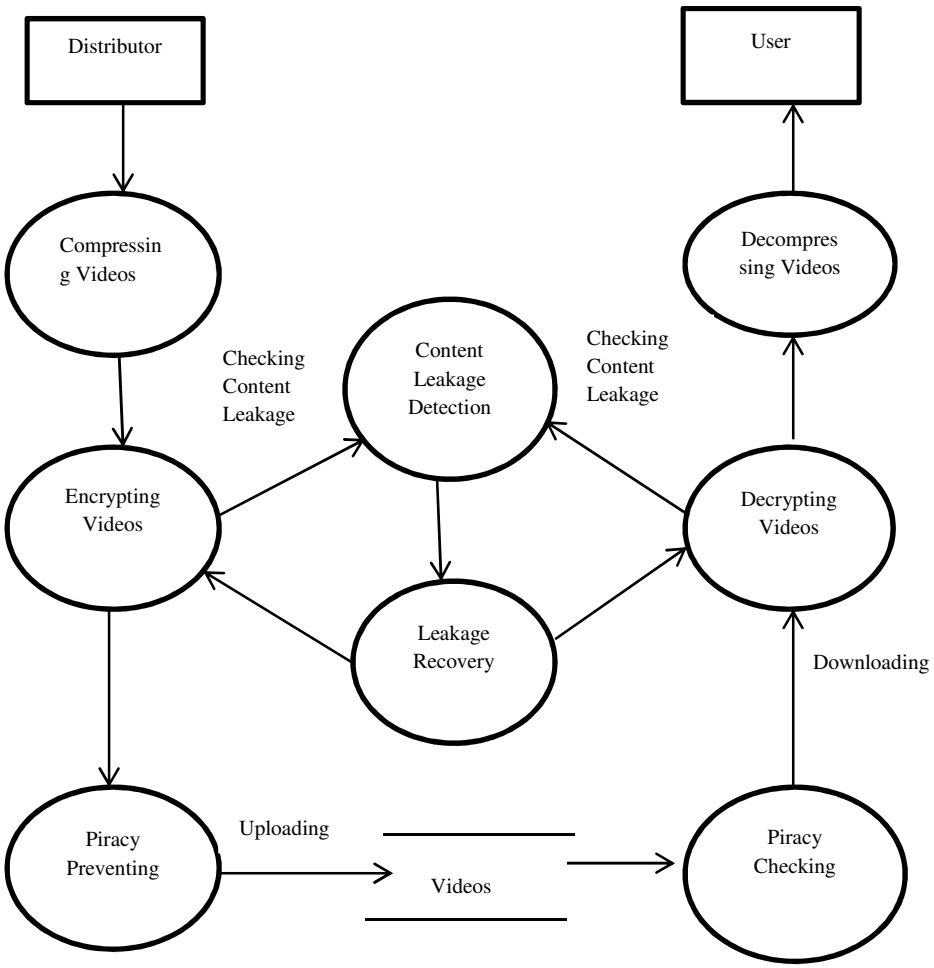

Figure 2. Dataflow Diagram for Overall Design

3.1 VIDEO COMPRESSION

Video is being compressed by arithmetic length encoding. The original videos are framed into 8 * 8 blocks. Then the blocks are segmented based on discrete cosine transform. By applying quantization videos is being compressed. To decompress the videos, inverse the

e-ISSN: 2349-9745
p-ISSN: 2393-8161

discrete cosine transforms. Apply quantization. With the help of decompressed algorithm such as arithmetic length decoding, original video can be obtained.

3.2 DIGITAL SIGNATURE

Pseudo code:

Token Generation

Input: Digital Receipt

Output: Encrypted Authorization Token T

If Receipt is invalid

Deny the request;

Else

λ= Decrypt (Receipt);

P = Observe (Requestor)

K = privatekeyRequest(p);

Token T = Ownersign(f,p,t_s);

Reply = { k,p,T_s, t}

SendToRequestor{ Encrypt(Reply)}

Endif

Digital signature is used to maintain piracy prevention in authorized content. First, both distributor and user are fully trusted. Their public keys are known to all videos. The piracy prevention consists of two integral parts: token generation and authorization verification. All videos are encrypted using the session key assigned by the transaction server at purchase time.

A token is a digital signature of a three tuple :{ endpoint, file ID, timestamp} signed by the private key of the content owner. Since bootstrap agent has a copy of the digital receipt sent by transaction server, verifying the receipt is thus done locally. The Decrypt (Receipt) function decrypts the digital receipt to identify the file .The Observe (requestor) returns with the endpoint address.

3.2.1 Piracy Prevention

Peer Authorization Protocol

Input : T = Token, t_s= timestamp, S = Peer signature

e-ISSN: 2349-9745
p-ISSN: 2393-8161

Φ(λ,p)=file index for file at end point p

Output: Peer authorization status

True – Authorization granted

False – Authorization Denied

The Owner Sign function returns with a token. Upon receiving a private key, the bootstrap agent digitally signs the file ID, endpoint address, and timestamp to create the token. The reply message contains a four tuple :{ endpoint address, private key, timestamp, token}.

After token is being generated, user send request to download a video. A download request include a token, file index, timestamp, and the digital signature. If any of the fields are missing, the download is stopped. A download user must have a valid token T and signature S. Two pieces of critical information are needed: public key and the endpoint address. It verifies both token T and signature S. Token also contains the file index information and timestamp indicating the expiration time of the token. The Parse (input) extracts timestamp, token, signature, and index from a download request.

3.3 CONTENT LEAKAGE

Due to upload of n number of videos, distributor finds content leakage in the network. Also when user downloads video from the server, the heavy traffic in network arises. It leads to packet loss, jitter and time delay. It leads to content leakage in downloading the videos. Hence it is necessary to solve content leakage.

Throughout the video streaming process, the changes of the amount of traffic appear as a unique waveform specifies to the content. Thus by getting this information retrieved in the network, the content leakage can be detected. Pattern generation algorithm is used to match the video from user‘s side and server ‘s side. Based on the time slot , the content leakage can be detected. By applying pattern matching algorithm, content leakage can be recovered.

3.4 CONTENT LEAKAGE RECOVERY

Content can be recovered by determination of the decision threshold for detecting leakage. The steps of content recovery are as follows.

1. Threshold determination process

2. Comparison based on traffic pattern

3. Cost evaluation

In threshold determination, from the original video a portion of video being taken and generate the corresponding traffic pattern. These patterns are compared with the original traffic pattern to perform sampling of the length of the videos. Then the curve is being generated from the observed traffic pattern. It is necessary to compare the adjusted degree of similarity to the

e-ISSN: 2349-9745
p-ISSN: 2393-8161

decision threshold to the original video and recover the leakage. Then the cost is being evaluated for the above process.

VI. CONCLUSION AND FUTURE WORKS

The content leakage of video is being detected and piracy prevention has been proposed for the compressed videos. In future it may be enhanced to detect content leakage for online video conferencing.

REFERENCES

[1] Xiaosong Lou, Kai Hwang, "Collusive Piracy Prevention in P2P Content Delivery Networks" IEEE TRANSACTION ON COMPUTERS, VOL 58, NO. 7,JULY 2009.

[2] Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah, and NeiKato,"Traffic Pattern Based Content Leakage Detection for Trusted Content Delivery Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 301-309, Feb. 2014.

[3] Y. Liu, Y. Guo, and C. Liang, "A survey on peer-to-peer video streaming systems,"Peer-to-Peer Networking and Applications, Vol.1, No.1, pp.18- 28, Mar. 2008.

[4]M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Traitor Tracing Technology of Streaming Contents Delivery using Traffic Pattern in Wired/Wireless Environments," in Proc. IEEE Global Telecommunications Conference, pp.1-5, San Francisco, USA, Nov./Dec. 2006.

[5]Z. Yang, H. Ma, and J. Zhang, "A dynamic scalable service model for SIP-based video conference," in Proc. 9th International Conference on Computer Supported Cooperative Work in DE.

[6]O. Adeyinka, "Analysis of IPSec VPNs Performance in A Multimedia Environment," School of Computing and Technology, University of East London.

[7]http://www.lunarpages.com/uptime/importance-videos-business

[8]http://goanimate.com/video-makertips/why-video-marketing-important

[9]http://www.onemarketmedia.com/2011/01/03/51-ways-to-use-web-video-to-help-your-business-grow/

[10]http:/en.wikipedia.org/wiki/Shared_resouce

