JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Video Transcoding and Encryption with License Server

[1]Prince Kumar Singh, [2]Ms. Ruchika Aggarwal

[1]M.Tech in Computer Science & Engineering, [2]Associate Professor (CSE Deptt.)
[1]Department of Computer Science & Engineering,
[1]J.C Bose University Of Science And Technology, YMCA, Faridabad, Haryana

Abstract : **With the rapid increase and advancement of digital video streaming, reliable video processing and its security have become significant tasks. Despite the fact that there are several techniques and service providers, they are costly and do not provide a reliable antipiracy solution in terms of video security. Video content that is stored and transmitted over the internet might contain sensitive information, so there is an urgent need for an efficient and reliable solution for video processing and authenticated distribution. To address this need, this research paper focuses on exploring video transcoding, encryption, and licensing mechanism which makes it a stronger, more reliable, and more cost-effective solution.**

Keywords **- Video Transcoding, Video Encryption, AES, License Server, Anti Piracy, Video Security.**

I. INTRODUCTION

Today, there is a significant increase in video content, driven by digital platforms and the advancement of technology. It is playing an important role in every industry, whether it is education, corporate, social media, or the movie industry. One of the best examples will be the education industry, where teachers are teaching their students online with the distribution of on-demand and live video streams. So with the adaptation of digital video streaming, there is a need for a reliable and cost-effective video processing solution. Although there are many solutions and service providers providing such solutions, they are very costly, and somewhere their video security mechanism has less efficiency. However, with increased accessibility, the risk of unauthorised access to video content has also increased. Therefore, video content owners need to secure their video content. To address this need, we've developed video processing and security mechanisms that are reliable and cost-effective.

Video transcoding is the process of converting a video file from one format to another with different resolutions, bitrates, and codecs. This process ensures that the video can be played on different devices and network conditions, optimising the user's experience. Video encryption, on the other hand, is the process of transforming the video data into an unreadable format to protect it from unauthorised access. This process ensures that only authorised users can access the video content, preventing piracy and copyright infringement.

We propose a video transcoding and encryption system that uses a license server for secure video distribution. The system receives a video file, transcodes it to multiple formats, and encrypts it using AES with a unique key. The use of a license server allows content owners to control access to their content by licensing and distributing keys to authorised users. By combining these technologies, we can create a secure and efficient system for video transcoding and encryption that protects against unauthorised access and ensures licensing compliance.

II. PROPOSED SYSTEM

The proposed system comprises three main components: a video transcoding module, an viideo encryption module, and a license server.

2.1 Video Transcoding Module

The Video Transcoding Module's primary function is to convert video files from one format to another, enabling compatibility with various devices, network conditions, and streaming platforms. The module employs advanced video transcoding techniques to optimise the video files for efficient playback and delivery.

The Video Transcoding Module operates on the input video files, which can be in different formats, resolutions, bitrates, or codecs. It analyses the characteristics of the input files and applies appropriate transcoding parameters to generate output files in the desired formats. This ensures that the transcoded videos are compatible with a wide range of devices, including smartphones, tablets, smart TVs, and desktop computers.

During the transcoding process, the module performs tasks such as:

1. **Format Conversion**: It converts the video files from one format to another, such as MP4 or MKV to M3U8 (HLS) or DASH, based on the requirements of the target devices or streaming platforms.
2. **Resolution and Aspect Ratio Adjustment**: It adjusts the resolution and aspect ratio of the video files to match the capabilities of the target devices or desired streaming quality.
3. **Bitrate Optimisation**: It optimises the video bitrate to ensure efficient streaming and playback, considering factors such as network bandwidth, device capabilities, and desired video quality. This helps minimise buffering and ensure smooth video playback across different network conditions.
4. **Metadata Preservation**: It ensures that essential metadata associated with the video files, such as title, duration, subtitles, and audio tracks, are preserved during the transcoding process.

The Video Transcoding Module plays a vital role in ensuring the compatibility and optimised delivery of video content across various devices and streaming platforms. It enhances the user experience and enables seamless playback of video content.

2.2 Video Encryption Module

The Video Encryption Module's uses AES Encrption to provide strong encryption for the video files, ensuring the confidentiality and integrity of the content during storage and transmission.

During the encryption process, the module performs the following tasks:

1. Key Generation: It generates a encryption key that is used to encrypt and decrypt the video files. The key is typically generated using a strong random number generator.
2. Key Rotation: It involves periodically change of the encryption keys used for encrypting and decrypting the video files. It provides an additional security by limiting the exposure of a single encryption key.
3. Encryption: Using the generated encryption key, it applies AES encryption to the video files, transforming the data into ciphertext. AES operates on fixed-size blocks of data, typically 128 bits, and applies a series of complex mathematical operations, including substitution, permutation, and mixing, to obfuscate the data.

The AES Encryption ensures that the video content remains protected from unauthorised access, as the encryption key is required to decrypt the data successfully. It offers a high level of security and confidentiality for the video content, making it extremely difficult for unauthorised users to access or tamper the data without the encryption key. This ensures that the video files are securely stored and transmitted, maintaining the trust and integrity of the content throughout the distribution process.

2.3 License Server Module

The License Server acts as a central authority responsible for managing and granting licenses to authorised users, enabling controlled access to the encrypted video content. The License Server ensures that only authenticated and authorised requests can decrypt and view the protected video files.

The License Server performs the following key functions:

1. User Authentication: When a user requests access to the encrypted video content, the License Server authenticates their identity. This authentication process may involve verifying user credentials, such as username and password, cookie or token based authentication.
2. License Generation: Upon successful authentication, the License Server generates a license for the user. The license includes the necessary information, such as the decryption key or token, permissions, and access restrictions associated with the specific video content. The license is encrypted and securely delivered to the user. It cannot be decrypted on the fly by any unauthorised user.
3. License Validation: When a user attempts to decrypt and view the video content, the License Server validates the received license. It verifies the integrity and authenticity of the license, ensuring that it has not been tampered with or altered. This validation process prevents unauthorised modifications to the license and unauthorised access to the video content.
4. Access Control: The License Server enforces access control policies based on the permissions and access restrictions defined in the license. It verifies that the user has the necessary rights to access the specific video content, ensuring that only authorised individuals can decrypt and view the content.
5. License Revocation: In the event of a security breach or violation of license terms, the License Server has the capability to revoke licenses. This prevents further unauthorised access to the video content by invalidating the compromised license. Revocation may be triggered manually by administrators or automatically based on predefined rules and conditions.
6. License Expiration and Renewal: The License Server manages the expiration of licenses and handles the renewal process. It tracks the validity period of licenses and provides notifications or prompts for users to renew their licenses when necessary. This ensures that authorised users can continue to access the video content while maintaining control over the duration of access.

The License Server plays a critical role in controlling access to the encrypted video content, ensuring that only authorised users with valid licenses can decrypt and view the content. By effectively managing licenses, enforcing access control, and facilitating authentication and authorization processes, the License Server safeguards the content against unauthorised distribution and piracy.

III. PRACTICAL IMPLICATIONS

The proposed system of video transcoding, AES encryption, and license server integration holds several practical implications for the digital media industry.

3.1 Enhanced Content Protection

By combining video transcoding and AES encryption, content creators and distributors can ensure that their valuable video assets remain protected from unauthorized access and distribution. The robust encryption provided by AES adds an additional layer of security, making it difficult for hackers and pirates to decrypt and distribute the content illegally.

3.2 Secure Content Distribution

The integration of a license server enables controlled access to the encrypted video content. Authorized users are granted licenses, which include unique decryption keys, allowing them to securely access the content. This ensures that only authorized individuals can view the content, reducing the risk of piracy and unauthorized distribution.

3.3 Flexibility and Compatibility

Video transcoding enables the conversion of video files into multiple formats, resolutions, and bitrates, catering to different devices and network conditions. This flexibility ensures that users can access the content on various platforms, including smartphones, tablets, and smart TVs, while maintaining optimal video quality.

3.4 Business Opportunities

The deployment of the proposed system opens up new business opportunities for content creators, distributors, and streaming platforms. By offering secure and high-quality video content, they can attract a larger user base, retain subscribers, and potentially negotiate licensing agreements with content owners who seek reliable content protection measures.

IV. CONCULSION

Video transcoding enables accessibility of video content for a wide range of devices and platforms operating with different network bandwidths, leading to a better user experience during playback, while video encryption with a license server enables secure playback and distribution of video content to authorised users only, which minimises the risk of piracy of video content for content owners.

Video Transcoding and Encryption with License Server: This proposed system provides a comprehensive solution for reliable video processing and secure distribution. It is a cost-effective solution independent of any external service provider and much more secure with License Server. Video content owners can rely on this solution for their video distribution over the internet because of its operational simplicity and robust security.

V. FUTURE WORK

The security of video content distributed over the internet has endless scope for research and development. To tackle video content security and piracy, regular application upgrades are necessary.

A few of the future scopes for such needs are:

1. WAF (Web Application Firewall) can be implemented to tackle regular attacks for unauthorised access to video content. The risk of unauthorised distribution of video content can be minimised using such measures.
2. Dynamic Watermarking with User Information can be implemented at the client player end to minimise the sharing of video content. Any screensharing or screenrecording can be prevented by using dynamic watermarking.
3. Secure Access for Video Files at the Storage End can be implemented to restrict unauthorised access to video files with security mechanisms like cookie-based authentication, token authentication etc.

REFERENCES

[1] Keshav S. Kadam, Prof. A. B. Deshmukh, “Video Frame Encryption Algorithm using AES”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 5 Issue 06, June-2016.

[2] Tameem Hameed Obaida**,** Abeer Salim Jamil, Nidaa Flaih Hassan, “A Review: Video Encryption Techniques, Advantages And Disadvantages”, Webology (ISSN: 1735-188X) , Volume 19, Number 1, 2022.

[3] S.Hemalatha, V.Hemamalini, S.Manimozhi, B. Revathi, S. Sridevi, “Improved Crypto Analysis for Scrambling Digital Video Using Secret Key” International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2015.

[4] M. Abomhara, Omar Zakaria, Othman O. Khalifa, “An Overview of Video Encryption Techniques”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010, 1793-8201.