

Chapter 7

An End-to-End Video Content Encryption Module for HLS Video Streaming

Kazim Rizvi

Vellore Institute of Technology, India


Bhavisha J. Dholakia

Vellore Institute of Technology, India

Aditya Kaushik

Vellore Institute of Technology, India

Aswani Kumar Cherukuri

 <https://orcid.org/0000-0001-8455-9108>

Vellore Institute of Technology, India

Chandra Mouliswaran S.

Vellore Institute of Technology, India

ABSTRACT

For an individual or a small organization, protecting and securing content could be a new and challenging task. The existing options do not completely fulfill the demands for today's content consumption and security while providing a good customer experience. The authors came across this problem of content security as a small group while building an application and tried to find a simple solution to secure content for playback on Android, so that the end users would be able to stream seamlessly and without any hindrance caused due to the enhanced security. They explore the way of securing video content through AES and using HLS to enable streaming of those video files over the internet. At the client's end, they have used Google's exoplayer to decrypt the data and play it directly after authentication and authorization. They performed a comparative analysis of the current models with the given model of securing content. Overall, with the aim to create an end-to-end module, they show how all the elements interact and work together as a system to provide protection against external threats.

DOI: 10.4018/978-1-7998-8367-8.ch007

INTRODUCTION

Nowadays, the most popular type of content being consumed is videos. With around 1 billion hours of video content being watched from only YouTube, and based on the studies (<https://www.bento4.com/documentation/mp42hls/>) showing us that 32 percent of the total people consuming video content on a daily basis and 72 percent of the total videos coming from a video website or app, we can clearly state that the security of the content becomes a priority and in the near future, with the introduction of various social video applications such as tiktok, this demand is going to rise very high. In this kind of a situation, security is always an integral part. Small startups and individuals who cannot invest in building huge architectures need a simple solution to ensure the safety and security of the content in their applications.

One of the best ways of securing data is using cryptography to make it accessible to only those people who are authorized to do so. For this project, we explored various symmetric encryption algorithms based on their speed and efficiency and found that AES outperformed compare to all others in case of encryption as well as decryption. (Chakraborty, Dev & Naganur, 2015).

The comparative study between symmetric and asymmetric encryption provides us the details about the difference between the two types of algorithms on the basis of speed, complexity, nature, vulnerabilities etc. (Kumar, Munjal & Sharma, 2011; Maqsood, Ahmed, Ali & Shah, 2017). In terms of security, speed, effectiveness and possible attacks the comparison between symmetric algorithms, Princy (2015) have showed good results for blowfish and AES. After analysis of these studies we concluded that, in this case, AES would be the right algorithm for the encryption and decryption of huge files because of the lesser decryption time which eventually would result in a better user experience while providing security at the same time.

HLS stands for HTTP Live streaming protocol. It has been developed by Apple (<https://developer.apple.com/streaming/>) and was released in 2009. HLS protocol divides the video content into chunks of small videos that are further streamed over HTTP. One of the main features of HTTP streaming protocols like HLS and DASH is adaptive bitrate streaming which enables the user to stream at different bitrates depending on the client's bandwidth (Jain, Shrivastava & Moghe, 2020). They allow multiple types of content consumption methods such as VOD and Live. Additional features of the HTTP streaming protocols include switching streams, ad insertion and variable segmentation (Jugović & Banduka, 2017). The HLS works by downloading the master playlist once and then fetching the adapted streams. The delay between the client and server during an HLS live stream can be optimized using open source software such as FFmpeg (Kuchta & Miklošík, 2017). For the conversion of simple mp4, mpeg, etc video files to multiple segmented streams of .ts files and a manifest.m3u8 file, we can use libraries like Bento and FFmpeg (<https://www.bento4.com/documentation/mp42hls/>).

DRM (Digital Rights Management) is an approach to securing digital content and preventing unauthorized access. The basic need for a model of DRM includes encryption which provides the supplier to put constraints on the consumption of data (Mushtaq et al., 2017). The architecture of DRM involves a DRM server in between the client and the publisher which acts as a medium for authentication and sharing data between the two parties (Oyman & Singh, 2012). The comparison of multiple DRMs allows us to check their support on various client platforms and the type of content they deliver (Princy, 2015). The DRM model can be used for multiple applications too, such as in the healthcare industry, hence allowing our architecture to have a wide range of possible use cases in the real world (Sheppard, Safavi-Naini & Jafari, 2009).

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/an-end-to-end-video-content-encryption-module-for-hls-video-streaming/291163

Related Content

A Study of Product Development Engineering and Design Reliability Concerns

Daniel Aikhuele (2018). *International Journal of Applied Industrial Engineering* (pp. 79-89).

www.irma-international.org/article/a-study-of-product-development-engineering-and-design-reliability-concerns/202422

Group Technology

Zude Zhou, Huaqing Wang and Ping Lou (2010). *Manufacturing Intelligence for Industrial Engineering: Methods for System Self-Organization, Learning, and Adaptation* (pp. 189-213).

www.irma-international.org/chapter/group-technology/42626

Effective Strategies for Managing Communication in a Project

Murtadha Albuali (2021). *International Journal of Applied Industrial Engineering* (pp. 1-6).

www.irma-international.org/article/effective-strategies-for-managing-communication-in-a-project/276087

Hybrid Algorithms for Manufacturing Rescheduling: Customised vs. Commodity Production

Luisa Huaccho Huatuco and Ani Calinescu (2013). *Industrial Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 1488-1516).

www.irma-international.org/chapter/hybrid-algorithms-manufacturing-rescheduling/69351

Integration of the Internet of Things and Blockchain to Promote Collaboration in Smart Cities: A Case Study in China

Poshan Yu, Zixuan Zhao and Emanuela Hanes (2023). *Opportunities and Challenges of Industrial IoT in 5G and 6G Networks* (pp. 1-29).

www.irma-international.org/chapter/integration-of-the-internet-of-things-and-blockchain-to-promote-collaboration-in-smart-cities/324734