Chapter 1
Cloud-Based Content Distribution and Copyright Vulnerabilities

Srinivas Chippagiri
https://orcid.org/0009-0004-9456-3951
Independent Researcher, USA

ABSTRACT

The backbone of current digital content creation and distribution is cloud technology, which concomitantly raises emerging and complicated issues for copyright enforcement. Albeit the cloud allows scalable and global access to media, documents, creative assets, it also opens up the risk of unauthorized copying and redistribution of such content because of mis-configuration, loose control and the inherent openness of distributed systems. This chapter considers the cloud content lifecycle (namely ingestion, storage, delivery, and consumption) and provides analysis of the main threats that may compromise the intellectual property. Based on real-world case studies and examination of contemporary threats, the chapter presents the inadequacy of traditional Digital Right Management (DRM) in the cloud age and argues for the utilization of digital watermarking as an adjunct to provide forensic-grade rights enforcement, content tracking and tracing.

1. INTRODUCTION

The digital medium has shaped a new paradigm for content creation, distribution, and consumption. With the popularization of cloud services, a great change has arisen from physical, centralized model into decentralized and virtualized environment were distributed over places, devices, and networks. This shift has disrupted

DOI: 10.4018/979-8-3373-3785-2.ch001

sectors competing through the distribution of digital content, such as media and entertainment, publishing, education, software and enterprise knowledge management. But as these innovations have enabled the reach, efficiency, and personalization of the Web to date, they have also created new issues of trust and arbitrariness in our online content ownership and usage rights - and their enforcement.

At the heart of this revolution is on-demand, cloud-based content distribution, which allows users to search for and use digital content whenever they need it, where they need it. This paradigm utilizes cloud services (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)) to provide content through geographically dispersed data centers, content delivery networks (CDNs), and platform application programming interfaces (APIs).

The characteristics of cloud that provide excellent values – like data replication, auto-scaling, and global access – also undermine the traditional control or copyright enforcement mechanisms. Content 'After the Internet' Content (once the province of physical objects and distribution centers) now moves through the interconnected components of systems, frequently unbeknownst to the author or without the manifest consent of the creator (Tu et al., 2020).

Older methods of copyright protection — watermarking, licensing contracts, and takedown requests –were devised for more static and jurisdictionally-specific media systems. They do not well adapt to such dynamic transformation operations, edge node caches, adaptive stream slicing, or user generated content workflows used in the cloud.

One of the key challenges in this domain is the lack of control on the content visibility and lifecycle. This results in content being copied/stitched/transformed across services and regions in cloud platforms, with limited granular accounting and centralized control. A video uploaded for private viewing could be accidentally leaked through incorrect storage permissions or even accessed from areas that don't respect copyright.

As equally urgent is the threat of unauthorized access and dissemination. Weak authentication, credential leaks, and open APIs can be used by attackers or unauthorized personnel to get hold of high-value material. After obtaining this content, it can be downloaded, saved or further shared by more casual or criminal methods like P2P networks, unindexed sites, and messaging applications. Yet even premium level content - including corporate training videos, research papers and proprietary product documentation - can be leaked to the public domain, if they are not adequately secured. These leaks, in most cases, are not the product of complex technical breaks but of elementary slip ups, like shared logins, weak encryption, or not checking who has access to it.

In the face of these challenges, content providers and platform builders are exploring a set of technical and policy approaches. In this manner, digital watermarking may