


Chapter 2

Security Challenges in Cloud-Based Watermarking

Atul Agrawal


 <https://orcid.org/0009-0004-3601-3919>

ITS Engineering College, India

Shikha Verma

ITS Engineering College, India

Avinash Kumar Sharma

 <https://orcid.org/0000-0001-6762-6778>

Department of Computer Science and Engineering (CSE), Sharda School of Computing Science and Engineering (SSCSE), Sharda University, Greater Noida, India

Ashwani Kumar

 <https://orcid.org/0000-0002-2100-900X>

Bennett University, India

Mukesh Mann

Indian Institute of Information Technology, Sonapat, India

Pashupati Baniya

 <https://orcid.org/0000-0003-1951-4469>

IEC College of Engineering and Technology, India

ABSTRACT

Saving and securing digital assets in the cloud environment is a great concern due to the rapid growth of multimedia data and cloud computing. Digital watermark provides a powerful solution by identifying inaccurate brands in the digital content to verify and detect tampering. However, the use of watermarks in the cloud system introduces unique security risks, such as privacy violations, unauthorized access, and vulnerability to advanced attacks. This chapter presents a concentrated review of modern cloud-based watermark techniques, analyzing the trade-off between safety, performance and privacy. It examines methods in both spatial and transformational domains, discussing hybrid approaches using a cryptographic tool and evaluating their adaptability to cloud-specific dangers. To improve the strength, capacity and

DOI: 10.4018/979-8-3373-3785-2.ch002

invisibility of the watermark, ensure the user's privacy and calculation efficiency, the work identifies today's research interval and proposes future directions for safe and efficient watermarking in the distributed icing environment.

1. INTRODUCTION

Cloud-based watermarking has proven to be an important method of protecting digital assets and offers a scalable and cost-effective material safety solution in the dynamic digital ecosystem. Strong procedures for copyright protection, verification of ownership, and material authentication are now required due to the extensive use of digital materials and easy duplication and modification. (Tang et al., 2023). Because digital traits are unsafe for many risks, protective measures should be preferred. As a secret method of inserting data into digital media, watermark distributors and material manufacturers help to monitor how their work is used, and their intellectual property rights are protected (Zheng et al., 2021). To maintain the integrity and dependability of watermark methods, a separate set of safety problems should be solved by shifts in cloud settings. Although watermark authenticity can support claims, the question of liability in piracy is not immediately addressed. (Frattolillo, 2021). How easy is it to copy and change digital content (Yadav et al., 2020) on the security of intellectual property rights, resulting in the safety of intellectual property rights. A practical way to demonstrate the protection and authenticity of digital assets is through a digital watermark.

Scalability, accessibility and cost effects are only a few advantages of cloud-based watermarking, where watermark activities are performed on a Far server (Sharifara et al., 2013). By removing the need for local infrastructure and enabling watermarking services on request, the cloud-based strategy reduces operational overhead for material owners. However, there are some security risks associated with transferring sensitive data and watermarking processes to external cloud suppliers, which must be evaluated properly and minimized. Now it is easy to create and repeat digital content, including audio, videos and images, thanks to the increasing use of digital data as possible by improving internet technology and high-speed networks. Increasing concern about the preservation of copyright of digital content and commercial opportunities has expanded the digital watermarking industry. Cloud-based watermarks can address copyright problems, watermark attacks and safety problems by combining watermarks with hyperchaotic encryption (Li et al., 2020).

Data Privacy, data integrity and access to services are three main categories where security problems can be shared with cloud-based watermarks. Protect sensitive information from unwanted access, such as basic materials and watermarks, known as data privacy (Sujath and Satyanarayana, 2016). In the Ski context, data

26 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/security-challenges-in-cloud-based-watermarking/388655

Related Content

Modelling of the Cloud Service Quality Factors Using ISM

Rajesh Agarwal and Sanjay Dhingra (2022). *International Journal of Cloud Applications and Computing* (pp. 1-16).

www.irma-international.org/article/modelling-of-the-cloud-service--quality-factors-using-ism/295241

Quantifying the Resilience of Cloud-Based Manufacturing Composite Services

Mohammad Reza Namjoo, Abbas Keramati, S. Ali Torabi and Fariborz Jolai (2018). *International Journal of Cloud Applications and Computing* (pp. 88-117).

www.irma-international.org/article/quantifying-the-resilience-of-cloud-based-manufacturing-composite-services/213991

Mobile Cloud Computing: An Introduction

Jyoti Grover and Gaurav Kheterpal (2015). *Resource Management of Mobile Cloud Computing Networks and Environments* (pp. 1-23).

www.irma-international.org/chapter/mobile-cloud-computing/125958

Pervasive Pedagogy: Collaborative Cloud-Based Composing Using Google Drive

Maury Elizabeth Brown and Daniel L. Hocutt (2017). *Integration of Cloud Technologies in Digitally Networked Classrooms and Learning Communities* (pp. 98-119).

www.irma-international.org/chapter/pervasive-pedagogy/172265

A Practical Application of TrimCloud: Using TrimCloud as an Educational Technology in Developing Countries

Beatriz Adriana Gomez and Kailash Evans (2016). *International Journal of Cloud Applications and Computing* (pp. 37-48).

www.irma-international.org/article/a-practical-application-of-trimcloud/159850