Chapter 9

Real-Time Watermarking in Cloud-Edge Computing-Optimizing Latency and Security

Birendra Kumar Saraswat
https://orcid.org/0000-0003-0628-6823
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Tarun Kumar Sharma
ABES Engineering College, India

Anand Muni Mishra
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Ratnesh Kumar Shukla
https://orcid.org/0000-0002-8279-7011
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Naveen Kumar Singh
https://orcid.org/0009-0007-0749-3820
HRIT University Ghaziabad

ABSTRACT

The present era is witnessing the proliferation of data – primarily due to the Internet of Things (IoT) devices and intelligent applications – which is experiencing an exponential rise. As more industries move applications to the cloud and/or edge, they must find a way to protect sensitive information in multimedia data while implementing ultra-low latency processing. Real-time watermarking, in which imper-

DOI: 10.4018/979-8-3373-3785-2.ch009

ceptible identifiers or ownership marks are embedded within streams of data, is an attractive approach to addressing this problem. It not only guarantees data security and copyright protection but also maintains the speed and efficiency required for contemporary distributed systems. The concept of watermarking is not itself a new one; indeed, such techniques have been used in traditional copyright enforcement and tamper-detection schemes in static (offline) batch-processing environments.

I. INTRODUCTION

However, the rise of edge computing has drawn computing closer to data sources for real-time processing "at the edge," to minimize latency and bandwidth consumption. Incorporating watermarking into these heterogeneous cloud-edge architectures presents both challenges and opportunities. A key virtue of cloud-edge architectures is the proliferation of computation down to end-user devices. However, computationally intensive operations, such as watermarking, cause the processing latency to be overestimated. To tackle this, new watermarking algorithms are proposed for lightweight and progressive processing. These schemes utilize local edge nodes for in-situ embedding or detection, thereby eliminating the need for frequent round-trips to a central cloud node. For example, in medical imaging pipelines, each processing node may insert a timestamp, thereby chaining the complete history from generation to cloud storage and processing. Furthermore, integrating watermarking protocols with edge security mechanisms— e.g., TEEs and secure multi-party computation— also reduces the possibility of insider attacks or data loss. These schemes protect the watermarking process from the tampering itself. Moreover, privacy-preserving watermarking techniques can be introduced to ensure that the watermarked data and watermark do not disclose sensitive information to an adversary. Although the potential of real-time watermarking in cloud-edge systems is interesting, several challenges need to be addressed. Scalability is a challenge—distributed systems can encompass thousands of diverse nodes with varying computing capabilities, network links, and network conditions. Aligning watermarking criteria and test conditions for such dynamic, ever-changing networks is anything but easy. Similarly, adaptive watermarking methods need to be resistant to unfrozen edge workloads and possible adversarial attacks that could deprive or modify the embedded data. Future studies can focus on federated learning-based watermarking, collaborative watermark evolution, and blockchain support for a more secure watermarking registry and conflict arbitration. Energy-aware watermarking solutions for battery-constrained edge and quantum-secure watermark encodings for next-generation security are also expected to be increasingly considered. It can be observed that real-time watermarking in cloud-edge computing lies at the intersection of latency