Chapter 22
A Hierarchical Security Model for Multimedia Big Data

Min Chen
University of Washington Bothell, USA

ABSTRACT

In this chapter, the author proposes a hierarchical security model (HSM) to enhance security assurance for multimedia big data. It provides role hierarchy management and security roles/rules administration by seamlessly integrating the role-based access control (RBAC) with the object-oriented concept, spatio-temporal constraints, and multimedia standard MPEG-7. As a result, it can deal with challenging and unique security requirements in the multimedia big data environment. First, it supports multilayer access control so different access permission can be conveniently set for various multimedia elements such as visual/audio objects or segments in a multimedia data stream when needed. Second, the spatio-temporal constraints are modeled for access control purpose. Finally, its security processing is efficient to handle high data volume and rapid data arrival rate.

INTRODUCTION

Currently, multimedia including image, video, and audio accounts for 60% of internet traffic, 70% of mobile phone traffic, and 70% of all available unstructured data (Smith, 2013). It is considered as “big data” not only because of its huge volume, but also because of its increasingly imminent position as a valuable source for insight and information in applications ranging from business forecasting, healthcare, to science and hi-tech, to name a few. Due to the explosion and heterogeneity of the potential data sources that extend the boundary of data analytics to social networks, real time streams, and other forms of highly contextual data, security assurance becomes one of the critical areas in this big data environment, which implies that the data be trustworthy as well as managed in a privacy preserving manner (Bhatti, LaSalle, Bird, Grance, & Bertino, 2012).

In the literature, many studies have been conducted to address security issues in the big data environment using approaches such as role management and access control (Choi, Choi, Ko, Oh, & Kim,

DOI: 10.4018/978-1-4666-9840-6.ch022

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

2012; Nehme, Lim, & Bertino, 2013) and have achieved promising results. However, several security requirements caused by special properties of multimedia big data are not yet well addressed and access control enforcement, the ability to permit or deny a request to perform an operation, is considered one of the most challenging and important aspects in multimedia big data (Nehme et al., 2013). Some main challenges are summarized below:

1. Many existing security models mainly focus on protecting documents on the file-level (Bertino, et al., 2003; Zhao, Chen, Chen, & Shyu, 2008). However, multimedia data often consists of a huge number of elements with different level of "sensitivity." For example, patients' personal information in a medical archive, a vehicle plate number in a car image or a victim's face in a surveillance video often requires a higher level security protection than other general elements. Therefore, the security mechanism must be flexible and able to support multilevel access control so it is convenient to set different access permission for various visual/audio objects or segments in a multimedia data stream when needed;
2. Besides multimedia contents being multi-level and dynamic, users' access privileges may also change due to their mobility when they try to access data from different places, at different time, and using different devices (Kulkarni & Tripathi, 2008). For example, a doctor may only be allowed to access certain medical images through computers inside the hospital local network when on duty, not the computers at home or when off duty. Therefore, the security mechanism should take into consideration of the spatio-temporal constraints and model them in a coherent manner;
3. In a multimedia big data environment, many applications, such as patient monitoring, location-based support system, etc., use large amount of real-time data to ensure high quality services where efficiency is of ultimate importance besides security assurance (Nehme et al., 2013; Sachan, Emmanuel, & Kankanhalli, 2010). Therefore, the security mechanism should be able to handle high data volume and rapid arrival rate, and security processing can be done on-the-fly or more realistically faster than the data incoming speed.

Though multimedia standards like MPEG-7 offers a comprehensive set of audiovisual description tools to describe multimedia contents, the security requirements are left open without the mechanism to specify who is allowed to access which (parts of the) multimedia data under which mode (Pan & Zhang, 2008). Therefore, it is essential to support security management of multimedia big data and design security models accordingly.

In this paper, a hierarchical security model (HSM) is proposed to address all these challenges. It provides role hierarchy management and security roles/rules administration, which extends the traditional role-based access control (RBAC) by adopting the object-oriented concept, spatio-temporal constraints, as well as taking into consideration and making full use of the multimedia standard MPEG-7.

The rest of the paper is organized as follows. First a literature review is conducted on the security access control models for multimedia big data and MPEG-7 properties that can be used to extend RBAC. Then the proposed hierarchical security model is presented followed by a performance evaluated using two example scenarios. Finally, the paper is concluded.

11 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/a-hierarchical-security-model-for-multimedia-big-data/150178

Related Content

Data Mining in Information Technology and Banking Performance
Yao Chenand Joe Zhu (2003). *Data Mining: Opportunities and Challenges (pp. 382-394).*
www.irma-international.org/chapter/data-mining-information-technology-banking/7610

Data Mining Techniques for Communities’ Detection in Dynamic Social Networks
Céline Robardet (2013). *Data Mining: Concepts, Methodologies, Tools, and Applications (pp. 719-733).*
www.irma-international.org/chapter/data-mining-techniques-communities-detection/73467

Fuzzy Miner: Extracting Fuzzy Rules from Numerical Patterns
Nikos Pelekis, Babis Theodoulikis, Ioannis Kopanakisand Yannis Theodoridis (2005). *International Journal of Data Warehousing and Mining (pp. 57-81).*
www.irma-international.org/article/fuzzy-miner-extracting-fuzzy-rules/1748

Case Studies on the Use of Data Mining Techniques in Data Science
(2023). *Principles and Theories of Data Mining With RapidMiner (pp. 193-204).*
www.irma-international.org/chapter/case-studies-on-the-use-of-data-mining-techniques-in-data-science/323375

Multi-Label Classification: An Overview
Grigorios Tsoumakasand Ioannis Katakis (2007). *International Journal of Data Warehousing and Mining (pp. 1-13).*
www.irma-international.org/article/multi-label-classification/1786