A Multimedia-Based Threat Management and Information Security Framework

James B.D. Joshi

Dept. of Information Science and Telecommunications, University of Pittsburgh,

135 N. Bellefield Ave., Pittsburgh, PA 15260, USA

Phone: 412-624-9982, Fax: 412-624-2788, Email: jjoshi@mail.sis.pitt.edu

Mei-Ling Shyu

Department of Electrical and Computer Engineering, University of Miami

Coral Gables, FL 33124-0640, USA

Phone: 305-284-5566, Fax: 305-284-4044, Email: shyu@miami.edu

Shu-Ching Chen

School of Computer Science, Florida International University

Miami, FL 33199, USA

Phone: 305-348-3480, Fax: 305-348-3549, Email: chens@cs.fiu.edu

Walid Aref

Department of Computer Science, Purdue University

250 N. University St., West Lafayette, Indiana 47907, USA

Phone: 765-494-1997, Fax: 765-494-0739, E-mail: aref@cs.purdue.edu

Arif Ghafoor

School of Electrical and Computer Engineering, Purdue University

465 Northwestern Ave., West Lafayette, Indiana 47907-2035, USA

Phone: 765-494-0638, Email: ghafoor@ecn.purdue.edu

A Multimedia-Based Threat Management and Information Security Framework

Abstract

This chapter focuses on the key challenges in the design of multimedia-based scalable techniques for threat management and security of information infrastructures. It bring together several multimedia technologies and presents a conceptual architectural framework for an open, secure distributed multimedia application that is composed of multiple domains employing different security and privacy policies and various data analysis and mining tools for extracting sensitive information. The challenge is to integrate such disparate components to enable large-scale multimedia applications and provide a mechanism for threat management. The proposed framework provides a holistic solution for large-scale distributed multi-domain multimedia application environments.

INTRODUCTION

Security of information infrastructures, both in public or private sectors, is vital to the overall national security goals. Such infrastructures provide capabilities for gathering, managing, and sharing vital information among numerous organizations that can form large e-enterprises and generally interoperate in form of a federation of autonomous domains (Joshi, 2001; Thuraisingham, 2003). Information shared among multiple domains can come in various forms including text, audio, video and images which can increase the complexity of security and privacy management. The key security challenges include integration of diverse security policies of collaborating organizations into a coherent capability for protecting information and using collaborative knowledge for detecting and responding to any emerging threats. In addition, information privacy is generally an overriding concern (Adams, 1999). Furthermore, a plethora of data analysis and mining tools have emerged that cyber defenders can use to extract sensitive information from public and private multimedia applications and detect patterns and activities indicating potential threats to an infrastructure. Thus, two key challenges to the design of multimedia-based scalable techniques for threat management and security of information infrastructures are *data mining* and *security*, which we briefly overview in the next section.

KEY ISSUES IN DATA MINING AND MULTIMEDIA SECURITY

Multimedia Data Analysis and Mining

Emerging multimedia applications require large-scale integration, mining, and analysis of multimedia data that is generally distributed over multiple security domains. Most of these applications use sensitive information for identifying complex threat actions that cannot be detected via real-time monitoring as such actions can take place over relatively long timeframes. Examples of such applications include detecting spread of an epidemic and monitoring deterioration of environment. However, nowadays, data no longer appears only in the text form. Instead, the information from different sources may be in the form of text, image, video, audio, or multimedia documents consisting of several multimedia objects that are tightly synchronized both in space and time (Little, 1990). Unlike mining the relational data, multimedia data mining is a more complex issue due to the sheer volume and the heterogeneous characteristics of the data, and the spatial and/or temporal relationships that may exist among multimedia data objects.

Mining multimedia data has recently been addressed in the literature (Chen, 2003a; Chen, 2004c; Thuraisingham, 2003). Most of the existing approaches, however, provide limited capabilities in terms of content analysis and generally do not exploit correlations of multiple data modalities originated from diverse sources and/or sensors. Real-time mining and correlating of multi-modality data from distributed sources and using security-oriented spatio-temporal knowledge can assist in identifying potential threats and ensuring security of large scale infrastructures (e.g., in command and control environments). In a broader perspective, both *long-ranged* and *real-time* data analysis and mining techniques are needed to allow multi-level content analysis and representation of multimedia data at different levels of resolution to facilitate information classification that has security and privacy implications.

Security Policy and Privacy Management

The multimodality nature of data and the unique synchronization and *quality of service* (QoS) requirements of multimedia information systems makes its protection uniquely challenging. These challenges are briefly discussed below.

Content-based Context-aware Access. An application may require controlled access to information based on the sensitivity level of information content, time, location and other contextual information obtained at the time the access requests are made. For example, in the healthcare industry, selective content-based access to patient information should be given to physicians, insurance providers, etc. Furthermore, a non-primary physician of a patient, who normally does not have access to the patient's records, may need to be allowed access in a "*life-threatening*" situation.

Heterogeneity of Subjects and Objects. For multimedia applications, heterogeneity implies the diversity of object and subject types. Object heterogeneity implies different types of media, abstract concepts, or knowledge embodied in the information that needs to be protected. For instance, in a digital library system, it is desirable to provide access based on concepts rather than on individual objects. For example, a user may want to access information related to concept '*Juvenile Law*'. Subject heterogeneity implies that the users have diverse activity profiles, characteristics and/or qualifications that may not be known *a-priori*, which can complicate the specification of access control requirements.

Privacy. Because of the richness of information content of multimedia data, privacy concerns are exacerbated in a multimedia environment (Adams, 1999). For instance, a perfectly harmless video sequence of a conference presentation may show certain behavior of a person (e.g., sleeping during the presentation) in the audience which may result in adversely affecting his status if it is viewed by his employer.

Dynamically Changing Access/Privacy Requirements. Access control and privacy requirements in Web-based multimedia applications are inherently dynamic in nature, as the information contents may change frequently. Powerful and flexible access control and privacy models are needed to capture dynamically changing access and privacy parameters in an evolving system.

Integration of Access and Privacy Policies. As multimedia information often exists in distributed heterogeneous administrative domains, there is a growing challenge of developing efficient integration and evolution management tools and techniques for inter-domain access control policies for distributed multimedia applications. Mechanisms are required to support careful analysis of security policies for the multi-domain environment and for mapping multimedia content parameters associated with the *security clusters* that data mining tools may generate to define content based access control and privacy policies. Situations can also arise when the existing static security policies, both local and global, may not provide sufficient safeguards against emerging threat scenarios and require changes as a scenario unfolds based on the information extracted from newly mined data. In such situations, real-time analysis of dynamic access control policies is required to prevent any potential breaches in the security in multimedia applications. In such an integrated environment, another key challenge is to efficiently manage the evolution of local and global information classifiers, and security and privacy policies.

Central to these problems is a crucial issue of uniform representation, interchange, sharing and dissemination of information content over an open, multi-domain environment. Due to the multimodality nature of multimedia data, the real-time constraints and heterogeneity of distributed domains, an integrated solution is needed to address the above-mentioned data mining, and security and privacy challenges. To meet these requirements, the integration of several technologies such as data mining, distributed multimedia systems, access control, and privacy models and mechanisms is needed. *EXtensible Markup Language* (XML) (Bertino, 1999; Damiani 2002) has emerged as a promising technology for addressing such a fundamental issue of information representation, interchange, sharing and dissemination (Thuraisingham, 2001). XML supports a rich set of features including user-defined tags, nested document structures and document schemata (Bertino, 1999; Bertino, 2001b; Damiani 2002). Several emerging XML related technologies including *Resource Definition Framework* (RDF), *DARPA Agent Markup Language + Ontology Inference Layer* (DAML+OIL) and *Web Ontology Language* (OWL) provide the support for integrating information from different domains by facilitating semantic matching of elements (Hunter, 2003; McGuinness, 2002). Moving Pictures Experts Group's MPEG 21 is an open multimedia standard that supports multimedia content delivery and consumption (Burnett, 2003). MPEG-21, however, does not capture flexible access control requirements outlined earlier. To the best of our knowledge, no prior research has addressed the above issues in a unified manner by integrating various technologies for developing a secure distributed multi-domain multimedia environment, although several researchers have addressed some of these issues. In this chapter, we discuss various challenges and present a conceptual framework for a scalable secure multi-domain multimedia information system that addresses these challenges.

CONCEPTUAL SYSTEM ARCHITECTURE

Various functional components of the conceptual architecture for a single domain multimedia environment are depicted in Figure 1. The *XML-based Multimedia Document Composition Module* (XDCM) provides an interface for composing XML schemata for multimedia information and policy documents, and includes *Policy Composition Interface*. Access control and privacy policy documents are stored in the *XML Policy Base* (XPB). The *Access Control and Privacy Enforcement Modules* (ACM, PEM) constitute the key enforcement modules. The ACM employs a content-based context-aware RBAC engine, extracts the policy information from the XPB and interacts closely with the *XML View Generator* (XVG) module to produce the authorized presentation schema for a user. Authorized XML instances are further checked against privacy policies by the PEM to ensure that privacy policies are enforced. The *Session Management Module* (SMM) is responsible for monitoring real-time activities of the multimedia presentation as well as dynamic access constraints and interacts with ACM and XVG to update active XML views.

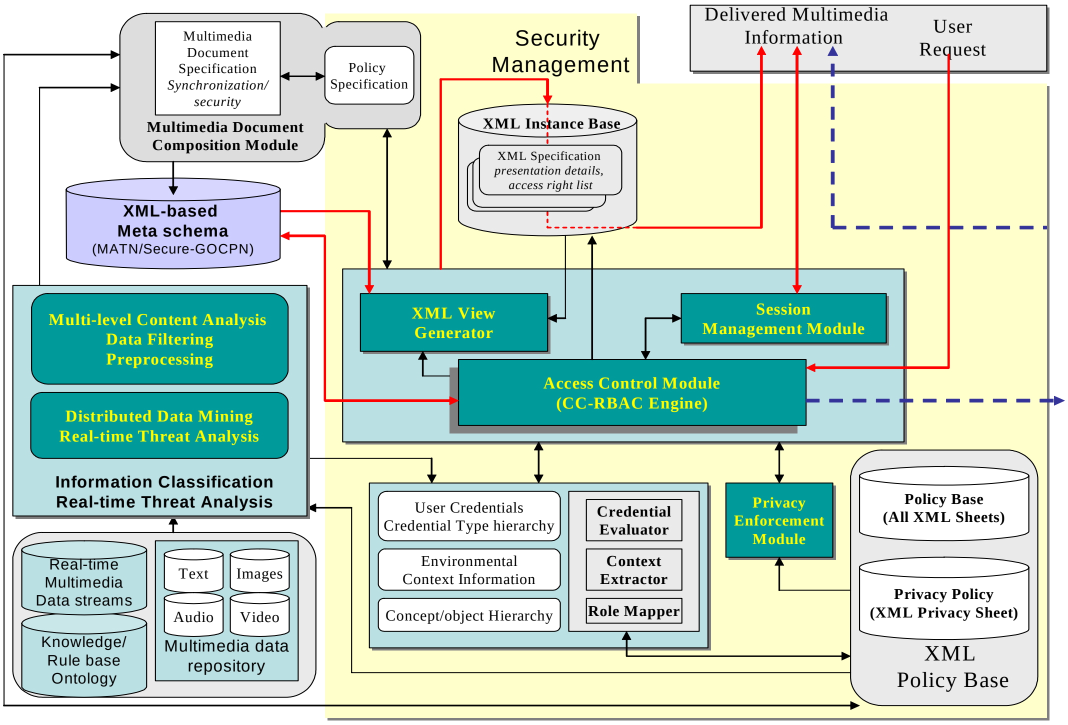
Multimedia Document Specification Synchronization/ security
Policy Specification
Multimedia Document Composition Module
Security Management
Delivered Multimedia Information
User Request
XML Instance Base
XML Specification presentation details, access right list
XML-based Meta schema (MATN/Secure-GOCPN)
Multi-level Content Analysis Data Filtering Preprocessing
Distributed Data Mining Real-time Threat Analysis
Information Classification Real-time Threat Analysis
XML View Generator
Session Management Module
Access Control Module (CC-RBAC Engine)
User Credentials Credential Type hierarchy
Environmental Context Information
Concept/object Hierarchy
Credential Evaluator
Context Extractor
Role Mapper
Privacy Enforcement Module
Policy Base (All XML Sheets)
Privacy Policy (XML Privacy Sheet)
XML Policy Base
Real-time Multimedia Data streams
Knowledge/ Rule base Ontology
Text
Images
Audio
Video
Multimedia data repository

Figure 1. Conceptual design of a single domain multimedia application environment

The *Information Classification and Real-time Threat Analysis Module* (ICRTAM) is responsible for the classification of multimedia data and threat analysis based on real-time multimedia data streams. The clusters that it generates are organized in a hierarchy. The *Role Mapper* generates concept roles for these clusters and creates required policy sheets that define access rules and privacy protection requirements. The *Credential Evaluator* (CEv) module evaluates the credentials presented by the ACM. With the help of the *Role*

Mapper, it maps the credentials to a role as defined by the access rules. The *Context Extractor* (CEx) evaluates the contextual information and sends the results to the ACM so it can evaluate context-based dynamic policies. The multimedia data repository constitutes the physical objects present in the system that are used to generate the XML multimedia object *meta-schema*, by integrating multimedia presentation information with security and privacy attributes. The *knowledge/rule base* or the *ontology* will be used by the information classification and security cluster generator module.

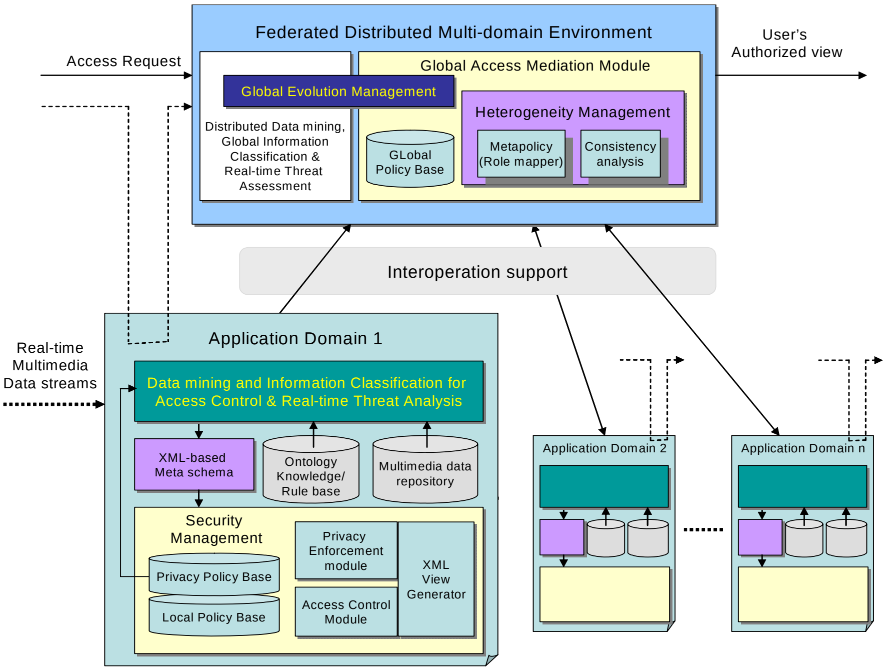
Federated Distributed Multi-domain Environment
Access Request
User's Authorized view
Global Access Mediation Module
Global Evolution Management
Distributed Data mining, Global Information Classification & Real-time Threat Assessment
GLobal Policy Base
Heterogeneity Management
Metapolicy (Role mapper)
Consistency analysis
Interoperation support
Real-time Multimedia Data streams
Application Domain 1
Data mining and Information Classification for Access Control & Real-time Threat Analysis
XML-based Meta schema
Ontology Knowledge/ Rule base
Multimedia data repository
Security Management
Privacy Policy Base
Local Policy Base
Privacy Enforcement module
Access Control Module
XML View Generator
Application Domain 2
Application Domain n

Figure 2. Conceptual design of a multi-domain multimedia application environment

The *Multi-level Content Analysis, Data Filtering and Pre-processing Module* (MCADFPM) is responsible for (*i*) conducting multi-level content analysis for mining and learning the semantic information; (*ii*) exploiting suitable multi-resolution representation schemes for various media features, segments, and objects; and (*iii*) enabling automatic feature selection to reach the compact sets of features and data set for data mining in the data-filtering and pre-processing step. The module assists in generating the security clusters and their attribute and feature sets. The *Distributed Data Mining and Real-time Threat Analysis Module* (DDMRTAM) is responsible for designing and developing (*i*) distributed data mining techniques for threat assessment based on real-time streams; and (*ii*) an information fusion model to resolve the inconsistencies when integrating the classification results from multiple local classifiers. The information clusters that it generates is organized in a hierarchy and represented in an XML.

Conceptual System Architecture for a Multi-domain Multimedia System

Figure 2 depicts the key components of the conceptual architecture of a secure federated distributed, multi-domain multimedia environment. The *Distributed Data Mining, Global Information Classification and Threat Assessment* component maintains global level views of conceptual objects based on the security clusters of individual domains. It also allows inter-site conceptual mapping of information objects, and distributes real-time threat assessment tasks with the help of the ontology or knowledge base of each domain. The *Global Access Mediation Module* integrates all the local policies into a unified *Global Policy Base*. The *Heterogeneity Management* module resolves any semantic differences and inconsistencies among the local policies when the global policy is constructed using the *Consistency Analysis* module. The final global level policy generated for the whole multi-domain environment primarily consists of a *Role Mapper* that maintains the mapping from global roles to local roles for access mediation. For a global access request, these mappings are used to issue access requests to individual domains. *Global Evolution Management* module is responsible for overseeing the process of ensuring consistent evolution of local information classification mechanisms and security/privacy policies.

SCALABLE MULTIMEDIA DATA ANALYSIS AND MINING TECHNIQUES

Content-based analysis of multimedia information for facilitating distributed security policies is a challenging issue because of the multimodality nature of multimedia data and heterogeneity of distributed information sources and sensors. Scalable real-time content-based analysis and mining frameworks are needed to generate security-oriented classification of multimedia information for the distributed multi-domain environment and to provide capabilities for real-time threat assessment. An efficient approach of real-time data stream querying across multiple domains is developed. A set of classifiers, both for individual domains and for global environment, that use a set of training data over relatively long timeframes is essential. Based on the semantics and the contents of information, these classifiers will produce a set of security clusters of multimedia objects each with a set of features and attributes that can be used for developing information security and privacy policies both for single and multi-domain environments, as discussed later. Another key challenge for designing the global classifier for multiple domains is to fuse information from local classifiers and resolve any semantic conflicts and inconsistencies in an efficient manner. Figure 3 depicts the data analysis and classification processes involved in multimedia information systems.

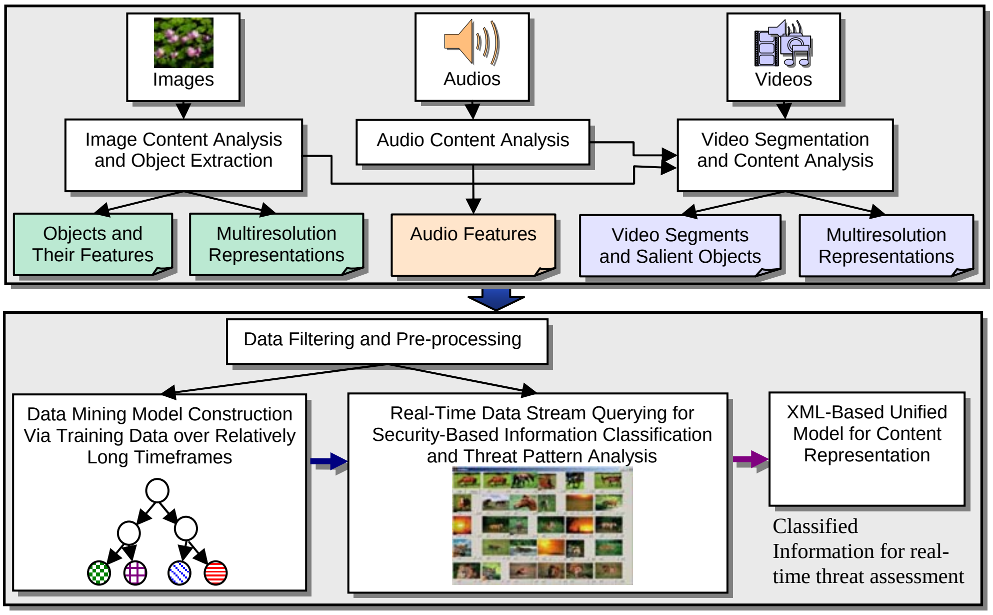
Images
Audios
Videos
Image Content Analysis and Object Extraction
Audio Content Analysis
Video Segmentation and Content Analysis
Objects and Their Features
Multiresolution Representations
Audio Features
Video Segments and Salient Objects
Multiresolution Representations
Data Filtering and Pre-processing
Data Mining Model Construction Via Training Data over Relatively Long Timeframes
Real-Time Data Stream Querying for Security-Based Information Classification and Threat Pattern Analysis
XML-Based Unified Model for Content Representation
Classified Information for real-time threat assessment

Figure 3. Architecture of multi-modal content data analysis and real-time data mining

Real-Time Content Analysis of Multi-Modality Multimedia Data. An in-depth content analysis and mining of multimedia data can provide tremendous wealth of information useful for security management and threat assessment. For this purpose, multi-modality content analysis is essential for integrating and transforming multimedia data into a format suitable for offline data mining model construction, and development of security clusters. Such analysis can span relatively long timeframes. On the other hand, data stream querying for classification and threat assessment requires real-time processing.

Multi-level Content Analysis of Multi-Modality Data. To automate multi-level real-time content analysis of multimedia data, a framework is needed that allows:

1. extraction of low-level features, including the color and shape features of an image or video frame, and the energy feature of an audio segment;
2. extraction of mid-level features, such as the object segmentation based on statistical features of the low-level features, and the video shot/scene segmentation;
3. extraction of high-level features that identify high-level multimedia content or events;
4. incremental learning to adapt to the changes in semantics over time.

Mining single-modality alone is not enough to reveal and interpolate the complex correlations of multiple data modalities from diverse sources. Therefore, it is more desirable to discover knowledge from multimedia data with multi-modalities and temporal relationships (Chen, 2003c; Chen, 2004a; Dagtas, 2001). A conceptually simple problem in information fusion is the combination of '*opinions*' of multiple classifiers. Several information fusion frameworks have been proposed, including the *Bayesian model, majority voting rule*, *average of classifier outputs*, *Naïve-Bayes*, *decision template,* and *dynamic classifier selection* (DCS) for integrating information from sources with different modalities (Giacinto, 2003; Krzysztofowicz, 1990).

Representation of Multimedia Data. Conventional multimedia database systems represent multimedia objects at the single level resolution. Multiresolution representation consists of maintaining multiple and concurrent representation of multimedia objects, and plays an important role in providing semantics to support access control and privacy of information. For example, a confidential medical X-ray image may also have the patient identity information. However, only the version without the identity information should be displayed to the unauthorized users. Multiresolution representation schemes for static images and video data based on the multisplines method have been proposed in (Moni, 1995), which has shown to yield excellent visual image quality. In addition, multiresolution representation provides an attractive solution in terms of coding complexity and image quality.

Real-Time Security-Based Information Classification and Threat Assessment. A set of suitable data mining classifiers, both for individual domains and for the distributed multi-domain environment, are required to support a comprehensive security framework. Such classifiers can be constructed offline using the training data over relatively long timeframes and used to generate information categorization for implementing the underlying content-based access control policies, with a wide range of classification parameters such as sensitivity level of information, its importance, and its semantics. In addition, real-time classifiers are needed to perform threat pattern analysis for detecting any emerging threats. The global classifier will integrate all the local classifiers and resolve the inconsistencies of the information among the local classifiers. These classifiers can generate security clusters consistent with access control and privacy management policies. Steps involved in the information classification process are discussed next.

Data Filtering and Pre-processing. The most challenging step prior to carrying data mining is to clean and prepare the data via data cleaning tools and/or domain-specific security knowledge or rules to ensure that the inputs of the data mining models are consistent with the overall security goals. The lack of a guide to choose the most appropriate sub-feature set can severely limit the effectiveness and efficiency of data pre-processing. Moreover, in cases when security knowledge is not available, selecting a subset of compact features can become a bottleneck, especially, when the features set is large. Several research works address this issue (Chen, 2003c; Dy, 2000; Shyu, 2003). A challenge is to develop efficient data cleaning and pre-filtering techniques by enabling automatic security and privacy policy driven feature selection, and eliminating unnecessary data records with the aid of domain knowledge.

Real-time Content Correlation of Multiple Streams for Event Detection. There exist no scalable mechanisms that can automatically correlate and synchronize multiple streams in multi-modalities and in spatial/temporal dimensions to support real-time data stream querying and event detection. Recently, a technique based on event-template for mining event information by combining audio and video cues to discover high level events in a medical database such as surgery and patient-physician dialogues in the context of a video database management system was proposed (Aref, 2003; Hammad 2003; Zhu, 2003).

Offline Data Mining Model Construction. Given the training data generated from the data filtering and pre-processing steps, another challenge is to develop a suitable, scalable data mining classifier that can generate relevant security clusters and their feature and attribute sets for implementing access control policies and identifying threat patterns. A data mining classifier is constructed offline by using the training data over relatively long timeframes. Generally, such classifiers can be used not only in evolving the existing threat patterns but also in discovering new threat patterns, which is extremely vital in real-time threat assessment. Conflicts and inconsistencies may arise while integrating information from multiple classifiers belonging to different domains into a global classifier, requiring information fusion to resolve these problems. A number of fusion rules can be used to combine individual classification generated by training local classifiers.

XML-based Unified Model for Content Representation. The security clusters identified by the data mining step will consist of complex multimedia objects, which usually come from multiple application domains and in multi-modalities, and hence a unified model for content representation is needed. One promising approach is to use XML for multimedia content representation and develop an XML-based meta-schema for the security clusters and their attribute and feature sets so that these clusters and their sets can be directly used for developing the security management component. In addition, the XML-based meta-schema will represent the multimedia composition schema for secure presentation instances that may be composed of text, audio, video and images. XML-based meta-schema is also used to represent the information retrieved by the data mining process and to identify multimedia documents and objects corresponding to the features and classes that the classifiers use, forming a high level conceptual "document."

DISTRIBUTED MULTIMEDIA SECURITY AND PRIVACY MANAGEMENT

The development of a fine-grained, content and context based access control and privacy model for multimedia applications raises a number of serious technical challenges. The privacy issue is a major concern in multimedia systems. Efficient techniques are required to generate correct mapping between the security and privacy requirements and the data analysis and classification mechanisms that generate security clusters. A unified XML-based language for expressing the security and privacy policies, as well as complex synchronization constraints can provide a basis for wider acceptance for practical use.

Access control may need to be applied at different levels of granularity and over hierarchically arranged multimedia objects. Few existing access control models address specific requirements of multimedia information system. Bertino *et al.* (2000a) proposed a video database access control model that allows access control at various levels of granularity of video information including video frames, video objects or a sequence. Joshi *et al.* (2002c) proposed a *Secure Generalized Object Composition Petri-net* (Secure-GOCPN) model by extending the GOCPN model of multimedia documents to support multi-level security policies by classifying multimedia information into a pre-specified set of classification levels. Subjects are also assigned security clearances that allow them to view information at or below a particular classification level. The unclassified level may correspond to preventing certain frames from being viewed by an unclassified user, or hiding sensitive information from each frame. Using the mapping of classification levels across multiple domains, an implementation architecture that supports the presentation of distributed multimedia documents that include media documents/objects from multiple sources was presented in (Joshi, 2002). The Secure-GOCPN model, however, only supports multilevel security policy. We propose using a role-based access control (RBAC) approach to address the generic security and privacy requirements of multimedia applications. RBAC supports fine-grained separation of duty (SoD) constraints, principle of least privilege, and efficient permission management. It also facilitates easy integration of policies because of the similarity of roles in different application domains (Ahn, 2000; Ferraiolo, 2001; Joshi, 2001; Kobsa 2003; Sandhu, 2000). Atluri *et al.* (2003) proposed a preliminary formal model of access control of multimedia information by enhancing Synchronized Multimedia Integration Language (SMIL) to express policies.

A parameterized RBAC Approach to Multimedia Information Systems. In an open environment such as the Web, a system should be able to facilitate a dynamic association of unknown users to a set of authorized actions. A content-based, context-aware RBAC framework would allow the users to be mapped to the activities authorized for them, based on context and credential information they present when requesting accesses. Roles also provide an abstraction level that can be used to capture security relevant features of multimedia objects, and the security clusters generated by data mining tools. To handle these issues, one approach is to use parameterized roles and role preconditions that will test the attribute and feature sets of the security clusters and multimedia objects being accessed, the credentials of the requester, and the contextual information that should be valid at the time of access. Along this direction, significant work has been done in temporal RBAC (TRBAC) model by Bertino *et al.* (2001a) and later in generalized TRBAC (GTRBAC) model by Joshi *et al.* (2005). Depending on the application semantics, not all roles may be available to all users at any time. This notion is reflected in the GTRBAC model by defining following states of a role: *disabled*, *enabled* and *active*. The *disabled* state indicates that the role cannot be activated in a session. The *enabled* state indicates that authorized users activate the role. A role in the *active* state implies that there is at least one user who has activated the role. Accordingly, the preconditions that change the states of a role are: (*i*) *role enabling/disabling precondition* to enable/disable a role; (*ii*) *role assignment/de-assignment precondition* to assign/de-assign a user (or permission) to the role; and (*iii*) *role activation/de-activation precondition* that specifies an authorized user can activate a role or when a role should be deactivated.

Though several researchers have addressed access control using parameterized roles, no formal model has been presented by any. One approach is to extend the event-based

GTRBAC model to develop a comprehensive event and rule-based, parameterized RBAC framework. A preliminary version of a parameterized role is presented in (Joshi, 2004b), which essentially builds on the event-based constraint framework of the GTRBAC model.

Extension of an XML Language for CC-RBAC Policies. We propose using an XML language that can express CC-RBAC modelling entities such as user credentials, role events and preconditions, clusters and multimedia objects and permissions associated with them by adopting the X-RBAC language proposed by Joshi *et al*. (2004b). A general credential expression of the form (*credTypeID, attributes*), where *credTypeID* is a credential type identifier and *attributes* is a set of attribute-value pairs, is used to map unknown users to predefined roles. In (Joshi, 2004), an XML-language for the basic RBAC model has been proposed to support parameterized RBAC policies. X-RBAC has been developed specifically for protecting XML content – *schema, instances,* and *elements*. The *schema, instances,* and *elements* of XML documents can naturally be extended to address the requirements of multimedia documents. Based on access control defined for the security clusters of multimedia objects and the presentation schema for such objects, presentation views for the users can be generated. Conceptual level access control policies use concept roles (Bhatti, 2003). It is possible that a schema element does not belong to the cluster to which its parent element belongs. It may further be necessary to specify that the element is not protected by a schema-level policy. At the lowest granularity, the protection may be applied to the fragments of an object such as on portions of a video sequence, and individual frames. The XML document structure for the specification of multimedia information also demands a specific set of privileges such as authoring a part of the XML document, modifying attributes only of a particular subset of the XML specification of a multimedia presentation, and navigating privileges to allow the use of links to navigate linked multimedia information.

Considerable amount of work on RBAC can be found in the literature (Ahn 2000; Ferraiolo, 2001; Sandhu 2000). Giuri et al. (1997) presented the concepts of parameterized privileges and role templates to allow the specification of policies based on the content of the objects. In (Georgiadis, 2001), the context of a team is composed of user context and object context. None of these studies address the consistency issues and complex requirements of multimedia applications. The environment roles in (Covington, 2001) are essentially statically defined context-roles and thus cannot be employed in a dynamic environment. In (Adam, 2002), a content-based access control (CBAC) model for a digital library has been proposed to protect the textual content of digital archives and uses credentials and concept hierarchies. Related work also includes several security mechanisms for schema and XML-instance level protection of XML documents (Bertino, 1999; Damiani 2002). Qin *et al.* (2003) recently proposed a content based access control model for Semantic web and used the concept level protection. These studies, however, do not address the security challenges in emerging multimedia applications mentioned earlier using an RBAC approach.

Privacy Protection in Multimedia Information Systems. In multimedia information systems, privacy concerns exist at multiple layers (Adams, 1999). At a primary level, privacy relates to the sensitivity of actual information content of the multimodal data. At the secondary level, it relates more to the socio-psychological characteristics of the data being accessed (Adams, 1999). For example, the clips about medical procedures may be used for teaching purposes; but if the clip shows a patient and his employer views it, it may have a detrimental effect, in particular, if the patient has a serious mental disease. While such multimedia clips may be of significant research value, appropriate measures need to be taken to ensure that privacy is protected. The three key factors of privacy protection are: *information sensitivity*, *information receiver* and *information use* (Adams, 1999; Jiang 2002). Privacy policies indicate who receives what level of private information for what use. A relevant issue is the inference problem (Thuraisingham, 2003). For instance, disease information may be inferred by collecting information on prescription data related to a patient. In particular, data mining can be used to infer facts that are not obvious to human analysis of data. In such cases, we need to protect private information that may be inferred.

A model for user privacy: In general, an application domain provides a privacy policy to protect user's private information that may have been maintained as historical profile or credential data collected for authorization purposes. (Ashley, 2002a; Tavani 2001; Jiang 2002). User consent is needed for releasing such private information to other parties. In particular, privacy requirements may need to be expressed as content-based and association-based constraints (Thuraisingham, 2003). A key challenge is thus to develop a privacy model and an enforcement mechanism that will be driven by the domain rules and user-controlled privacy policies. Suitability of several existing approaches to privacy management has not been applied to multimedia environments. The "*sticky policy*" based approach proposed in (Ashley, 2002a) uses privacy statements that "*stick*" to each piece of private information so that the privacy statements can be checked before the information is accessed. Another relevant approach uses privacy tags and defines an information space boundary (*physical*, *social* or *activity-based*) as a contextual trigger to enforce permissions defined by the owners of that space (Jiang, 2002). To address flexible privacy requirements in multimedia applications, these approaches may need to be combined, and the use of parameterized roles can provide significant benefits (Kobsa, 2003). One key issue is that when a user specifies a privacy policy the document itself becomes a protected object, and may conflict with the overall privacy policy of the domain.

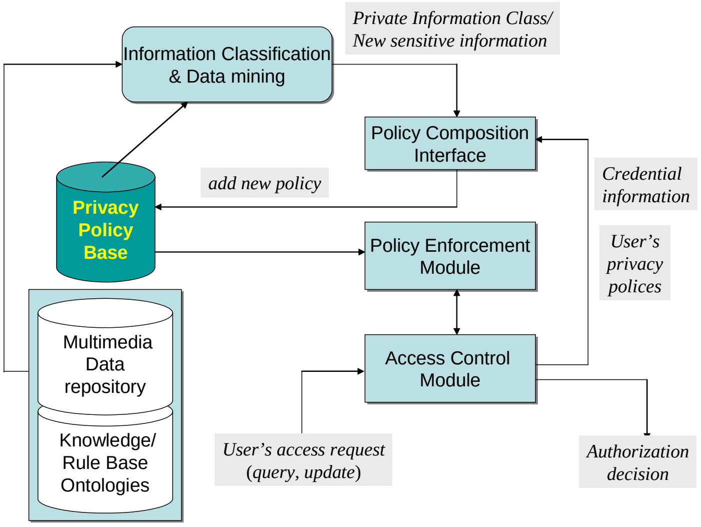

Figure 4. Privacy protection component

Privacy-aware information classification: To provide a fine-grained control over the release of private information, a mechanism is needed to provide the interaction between the data mining component that generates security clusters and the privacy protection module. Assume that a personal privacy policy states that "*None other than the concerned doctors should view any information that may reveal my disease*". Here, "*any information that may reveal my disease*" may simply be text containing prescription drug name, the disease name, or a video sequence showing the patient's physical features and indicating signs of the disease; and the "*concerned doctors*" is an abstract concept referring to a user group with certain characteristics. Meta-information from the privacy-policy base can be used as the domain knowledge for supporting the information classifiers at the time of generating security classes and their attributes and feature sets. Furthermore, data mining can reveal new sensitive and private information and associations that may not be possible through human analysis. For such information, if privacy statements do not exist, new privacy policies may need to be generated. Hence, the development of mechanisms that allow efficient interactions between the privacy protection and data mining modules is needed to iteratively refine both privacy policies and information classification. The overall privacy protection component in the proposed research is depicted in Figure 4. The access control module interacts with the privacy mechanism to ensure that privacy requirements are met before users can access data. Several privacy protection models and approaches have been discussed in (Jiang, 2002; Ashley, 2002a; Mont, 2003a; Tavani 2001; Kobsa, 2003; Adams, 1999).

Management of Secure Multi-domain Multimedia Information Systems

Heterogeneity is a uniquely complex challenge, as security and privacy policies and information classification methodologies may vary over all the domains giving rise to inconsistent inter-domain actions. The key challenges for developing secure distributed, multi-domain multimedia information systems are: (*i*) to identify conflicts among security and privacy policies, and (*ii*) to maintain a consistent global information classification.

The overall infrastructure for a secure distributed multi-domain multimedia application environment must allow seamless and secure interoperation among the diverse access control policies employed by each domain. Such an infrastructure should be scalable, open, and extensible (Joshi, 2001), and should allow any domain with an arbitrary security policy and information classification to be a part of the overall environment. An XML-based policy specification and enforcement framework can provide a more practical solution for secure interoperation in multi-domain multimedia environments.

In a multi-domain environment, individual domain policies may follow different conventions and use varying attributes. Semantic heterogeneity may give rise to naming or structural conflicts; a problem that is commonly encountered during schema integration in a heterogeneous federated database system (Batini, 1986). Naming conflicts occur due to the use of a single name to refer to different concepts. Known techniques from the integration of heterogeneous databases, and ontology can be utilized to resolve naming conflicts (Batini, 1986). Conflicts can also arise because of the differences in the representation of the similar constraints. In the CC-RBAC framework, the constraints can make the semantic heterogeneity issue even more difficult to address. It makes evolution management a significant problem.

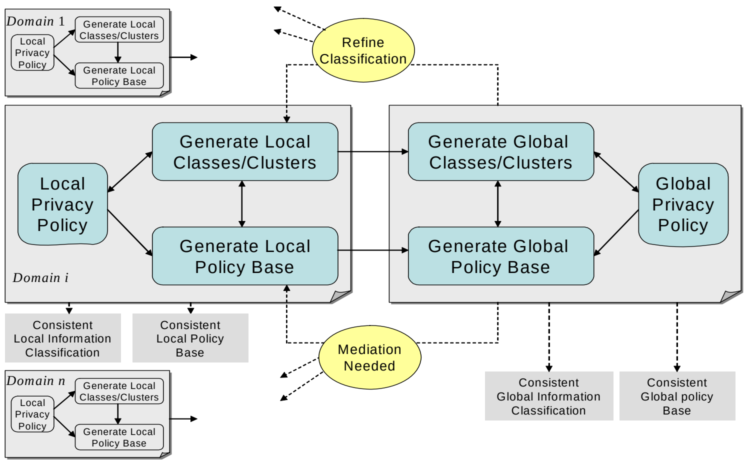
Domain 1
Local Privacy Policy
Generate Local Classes/Clusters
Generate Local Policy Base
Refine Classification
Local Privacy Policy
Generate Local Classes/Clusters
Generate Local Policy Base
Domain i
Generate Global Classes/Clusters
Generate Global Policy Base
Global Privacy Policy
Consistent Local Information Classification
Consistent Local Policy Base
Mediation Needed
Consistent Global Information Classification
Consistent Global policy Base
Domain n
Local Privacy Policy
Generate Local Classes/Clusters
Generate Local Policy Base

Figure 5.The integration process

Different application domains may use different data analysis and classification mechanisms to generate an equivalent set of concepts with different names or different concepts with similar names. At the global level, such semantic differences need to be properly resolved to ensure secure information access and privacy protection. In each application domain, there is an interaction between the information classification and policy generation modules as indicated in Figure 5. Once policies and information classification consistent to each other have been generated, the global level policy is generated. At the same time, a consistent global level classification also needs to be generated from local classifications. The global level policy and global level classification may be inconsistent if the local domains employ different classification schemes. To resolve such inconsistencies, local classifiers may need to be refined, which in turn affects the local policies. Hence, the global level policy generated earlier will now become inconsistent requiring further mediation of local policies. Such multi-dimensional horizontal and vertical interactions among the classification and policy generation modules at the two levels make the overall integration problem significantly complex. The challenge is to develop a framework for iteratively refining policies and information classes at the two levels. Local clusters/classes are extracted by data mining tools and are used as protection objects. Refinement of classifiers and mediation policies needs to be iterated until consistent classifications and policies are generated at each local domain as well as at the global level. The presence of dynamic and contextual roles can make the problem even more complex. Techniques are needed for detecting inconsistencies, automatically or semi-automatically, using attribute-based matching and ontologies. In particular, use of ontology to assist in semantic mapping between security policies of different domains is becoming a possibility because of the tools such as RDF, DAML+OIL and/or OWL. An ontology can be defined as "*the specification of conceptualizations, used to help programs and humans share knowledge*" (Hunter, 2003). Use of ontologies in the integration of security policies need to be similarly explored. In particular, for securing a distributed multi-domain application, use of ontologies related to the domain knowledge as well as the security policies and mechanisms of the individual administrative domains will be crucial to capture the names used to indicate various security attributes and their intended semantics and relationships.

Limited work has been done in the area of secure interoperation in a multi-domain environment. In (Shafiq, 2004), a policy composition framework for integrating simple RBAC policies to provide secure interoperation has been proposed, where RBAC constraints are transformed into an integer programming problem to optimize secure interoperation. In (Joshi, 2004b), the XML-based RBAC framework has been extended to specify arbitrary multi-domain policies. Integration of multiple policies has been focused generally on MAC mechanisms for federated database systems. Authors in (Thuraisingham, 1995) discussed methodologies for constraint processing in a multilevel, secure, centralized, and distributed database management system. In (Jonscher, 1995), the global access layer is used to map global authorizations into local access rights for the individual systems. XML-based tools to manage RBAC policies in an enterprise have been discussed in (Vuong, 2001).

CONCLUSION

In this chapter, we have presented a conceptual architectural framework for open, distributed multimedia information systems that aims at ensuring security and privacy of multimedia information and provides a mechanism for threat assessment. The proposed framework uses XML-technologies to address the needs for multi-resolution representation of multi-modal multimedia data, its storage, exchange and retrieval, as well as to develop access control and privacy specification. We have discussed the relevance of a content and context based RBAC approach to capture both the access control and privacy requirements of multimedia applications. The framework addresses the need for a holistic solution to supporting flexible access control and privacy requirements on multimedia information. Such information may contain sensitive and private data and can be analyzed to reveal patterns and knowledge for possible threats to an enterprise. The framework provides security and privacy protection, while facilitating real time and long-term analysis to detect potential threats.

REFERENCES:

Adams, A., & Sasse, M. A. (1999). Taming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications. ACM Multimedia 99. 101-106.

Adam, N. R., Atluri, V., & Bertino, E. (2002). A Content-Based Authorization Model for Digital Libraries. IEEE Transactions on Knowledge and Data Engineering. 14(2), 296–315.

Ahn, G., & Sandhu, R. (2000). Role-Based Authorization Constraints Specification. ACM Transactions on Information and System Security. 3(4), 207-226.

Aref, W.G., Catlin, A.C., Elmagarmid, A.K., Fan, J., Hammad, M.A, Ilyas, I., Marzouk, M., Prabhakar, S., & Zhu, X.Q. (2003). VDBMS: A Testbed Facility for Research in Video Database Benchmarking. ACM Multimedia Systems Journal, Special Issue on Multimedia Document Management Systems. Accepted 2003.

Ashley, P., Powers, C., & Schunter, M. (2002). From Privacy Promises to Privacy Management - A New Approach for Enforcing Privacy Throughout an Enterprise. ACM New Security Paradigms Workshop '02.

Ashley, P., Hada, S., Karjoth, G., & Schunter, M. (2002a). E-P3P Privacy Policies and Privacy Authorization. Proceeding of the ACM workshop on Privacy in the Electronic Society.

Atluri, V., Adam, N., Gomaa, A., & Adiwijaya, I. (2003). Self-Manifestation of Composite Multimedia Objects to Satisfy Security Constraints. ACM SAC. 927-934.

Batini, C., Lenzerini, M., & Navathe, S.B. (1986). A Comparative Analysis of Methodologies for Database Schema Integration. ACM Computing Surveys. 18(4), 323-364.

Bertino, E., Castano, S., Ferrari, E., & Mesiti, M. (1999). Controlled Access and Dissemination of XML Documents. Proceedings of the second international workshop on Web information and data management. 22– 27.

Bertino, E., Hammad, M.A, Aref, W.B., & Elmagarmid, A.K. (2000a). An Access Control Model for Video Database Systems. CIKM 2000. 336-343.

Bertino, E., Bonatti, P. A., & Ferrari, E. (2001a). TRBAC: A Temporal Role-based Access Control Model. ACM Transactions on Information and System Security. 4(3), 191-233.

Bertino, E., Castano, S., & Ferrari, E. (2001b). Securing XML Documents with Author-X. IEEE Internet Computing. 21-31.

Bhatti, R., Joshi, J.B.D., Bertino, E., & Ghafoor, A. (2003). XML-based RBAC Policy Specification for Secure Web-Services. IEEE Computer.

Burnett, I., De Walle, R.V., Hill, K., Bormans, J., & Pereira, F. (2003). MPEG-21 Goals and Achievements. IEEE Multimedia.

Chen, S.-C., Shyu, M.-L., Zhang, C., Luo, L., & Chen, M. (2003c). Detection of Soccer Goal Shots Using Joint Multimedia Features and Classification Rules. Proceedings of the Fourth International Workshop on Multimedia Data Mining (MDM/KDD2003), in conjunction with the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 36-44.

Chen, S.-C., Shyu, M.-L., Chen, M., & Zhang, C. (2004a). A Decision Tree-based Multimodal Data Mining Framework for Soccer Goal Detection. IEEE International Conference on Multimedia and Expo (ICME 2004).

Covington, M.J., Long, W., Srinivasan, S., Dey, A.K., Ahmad, M., & Abowd, G.D. (2001). Securing Context-Aware Applications Using Environmental Roles. 6th ACM Symposium on Access Control Models and Technologies. 10-20.

Dagtas, S., & Abdel-Mottaleb, M. (2001). Extraction of TV Highlights Using Multimedia Features. Processing of the IEEE International Workshop on Multimedia Signal.

Damiani, E., di Vimercati, S.D.C., Paraboschi, S., & Samarati, P. (2002). A Fine-Grained Access Control System for XML Documents. ACM Transactions on Information and System Security (TISSEC). 5(2), 169-202.

Dy, J.G., & Brodley, C.E. (2000). Feature Subset Selection and Order Identification for Unsupervised Learning. in Proc. 17th International Conference on Machine Learning. 247-254.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, R., & Chandramouli, R. (2001). The NIST Model for Role-Based Access Control: Towards a Unified Standard. ACM Transactions on Information and System Security. 4(3).

Georgiadis, C.K., Mavridis, I., Pangalos, G., & Thomas, R.K. (2001). Flexible Team-Based Access Control Using Contexts. 6th ACM Symposium on Access Control Models and Technologies. 21-27.

Giacinto, G., Roli, F., & Didaci, L. (2003). Fusion of Multiple Classifiers for Intrusion Detection in Computer Networks. Pattern Recognition Letters. 24, 1795–1803.

Giuri, L., & Iglio, P., (1997). Role Templates for Content-Based Access Control. Proceedings of the Second ACM Workshop on RBAC. 153-159.

Hammad, M.A, Franklin, M., Aref, W.G., & Elmagarmid, A.K. (2003). Scheduling for Shared Window Joins over Data Streams. The International Conference on Very Large Data Bases (VLDB), 297-308.

Hunter, J. (2003). Enhancing the Semantic Interoperability of Multimedia Through a Core Ontology. IEEE Transactions on Circuite and Systems for Video Technology. 13(1).

Jiang, X, & Landay, J.A. (2002). Modeling Privacy Control in Context-aware Systems. Pervasive Computing, IEEE. 1(3), 59–63.

Jonscher, D., & Dittrich, K.R. (1995). Argos – A Configurable Access Control System for Interoperable Environments. Proceedings of the IFIP WG 11.3 Ninth Annual Working Conference on Database Security. 39-63.

Joshi, J.B.D., Ghafoor, A., W. Aref, & E. H. Spafford (2001). Digital Government Security Infrastructure Design Challenges. IEEE Computer. 34(2), 66-72.

Joshi, J.B.D., Li, K., Fahmi, H., Shafiq, B., & Ghafoor, A. (2002c). A Model for Secure Multimedia Document Database System in a Distributed Environment. IEEE Transactions on Multimedia: Special issue of on multimedia databases. 4(2), 215-234.

Joshi, J.B.D., Bhatti, R., Bertino, E., & Ghafoor, A. (2004b). An Access Control Language for Multidomain Environments. IEEE Internet Computing. Nov-Dec 2004, pages 40-50

Joshi, J.B.D., Bertino, E., Latif, U., & Ghafoor, A. (2005). Generalized Temporal Role Based Access Control Model. IEEE Transaction on Knowledge and Data Engineering. 17(1), 4-23.

Kobsa, A., & Schreck, J. (2003). Privacy Trough Pseudonymity in User-adaptive Systems. ACM Transactions on Internet Technology (TOIT). 3(2).

Krzysztofowicz, r., & Long, D. (1990). Fusion of Detection Probabilities and Comparison of Multisensor Systems. IEEE Trans. Systems, Man, & Cybernetics. 20(3), 665-677.

Little, T.D.C., & Ghafoor, A. (1990). Synchronization and Storage Models for Multimedia Objects. IEEE Journal of Selected Areas in Communications, Special Issue on Multimedia Communication. 8(3), 413-427.

McGuinness, D.L., Fikes, R., Hendler, J., & Stein, L.A. (2002). DAML+OIL: An Ontology Language for the Semantic Web. IEEE Intelligent Systems.

Moni, S., & Kashyap, R.L.. (1995). A Multiresolution Representation Scheme for Multimedia Databases. Multimedia Systems. 3, 228-237.

Mont, M.C., Pearson, S., & Bramhall, P. (2003a). Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop. 377–382.

Qin, L., & Atluri, V. (2003). Concept-level Access Control for Semantic Web. ACM Workshop on XML Security.

Sandhu, R., Coyne, E.J., Feinstein, H.L., & Youman, C.E. (1996). Role-Based Access Control Models. IEEE Computer. 29(2), 38-47.

Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST Model for Role-Based Access Control: Toward a unified standard. in Proc. 5th ACM Workshop Role-Based Access Control. 47–63.

Shafiq, B., Joshi, J.B.D., Bertino, E., & Ghafoor, A. (2004). Secure Interoperation in a Multi-Domain Environment Employing RBAC Policies, IEEE Transactions on Knowledge and Data Engineering.

Shyu, M.-L., Chen, S.-C., Chen, M., Zhang, C., & Sarinnapakorn, K. (2003). Image Database Retrieval Utilizing Affinity Relationships. Proceedings of the First ACM International Workshop on Multimedia Databases (ACM MMDB'03). 78-85.

Tavani, H.T., & Moor, J.H. (2001). Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. ACM SIGCAS Computers and Society. 31(1).

Thuraisingham, B., & Ford, W. (1995). Security Constraints in a Multilevel Secure Distributed Database Management System. IEEE Transactions on Knowledge and Data Engineering. 7(2), 274-293.

Thuraisingham, B., Clifton, C., & Maurer, J. (2001). Real-Time Data Mining of Multimedia Objects. Fourth International Symposium on Object-Oriented Real-Time Distributed Computing. 360-365.

Thuraisingham, B. (2003). Web Data Mining Technologies and Their Applications to Business Intelligence and Counter-terrorism. CRC Press.

Vuong, N., Smith, G., & Y. Deng (2001). Managing Security Policies in a Distributed Environment Using eXtensible Markup Language (XML). Proc. 16th ACM Symposium on Applied Computing, 405-411.

Zhu, X.Q., Fan, J., Aref, W., Catlin, A.C., & Elmagarmid, A. (2003). Medical Video Mining for Efficient Database Indexing, Management and Access. In ICDE'03 Proceedings of the 19th International Conference on Data Engineering. 569-580.