Multimed Tools Appl (2007) 33:13–29
DOI 10.1007/s11042-006-0096-1

Security and privacy for multimedia database management systems

Bhavani Thuraisingham

Published online: 1 March 2007

Abstract This paper describes security and privacy issues for multimedia database management systems. Multimedia data includes text, images, audio and video. It describes access control for multimedia database management systems and describes security policies and security architectures for such systems. Privacy problems that result from multimedia data mining are also discussed.

Keywords Multimedia data management · Multimedia data security · Privacy · Security architecture · Secure data model · Security policy · Dependability · Data mining · Secure distributed multimedia data management

1 Introduction

Multimedia database management systems manage multimedia data including text, images, audio and video. More and more multimedia data are now available on the web and effective management of this data is becoming a critical need. We also need to ensure that the data is protected from unauthorized access as well as malicious corruption.

This paper will first discuss characteristics of multimedia database management systems and then discuss issues on incorporating security into such systems. It will review various security mechanisms and access control policies and discuss the applicability of these mechanisms and policies for multimedia data. It will discuss specific security challenges for text, imagery, audio and video data. Various security architectures for multimedia information systems will be examined. Trade-offs between real-time processing, security and data quality will be discussed. The paper will also discuss mining multimedia data

B. Thuraisingham (✉)
The National Science Foundation, Arlington, VA, USA
e-mail: bthurais@nsf.gov

B. Thuraisingham
MITRE Corporation, Bedford, MA, USA

management systems and examine the privacy violations that could occur through data mining.

Next we will examine the developments in digital libraries, which can be considered to be a special kind of multimedia information management systems, and discuss various developments on secure digital libraries. Access control models such as role-based access control and copyright protection method for digital libraries as well as secure information retrieval will be discussed. We will also examine the emerging developments in semantic web with respect to multimedia data and discuss issues in securing the semantic web. Extensions to languages such as XML (extensible Markup Language) and RDF (Resource Description Framework) for secure multimedia information management will be examined.

The organization of this paper is as follows. Background on multimedia data management and mining will be given in Section 2. Security for multimedia database systems including a discussion of discretionary security and multilevel security will be discussed in Section 3. Quality of Service for multimedia data management systems including tradeoffs between security, real-time processing and fault tolerance will also be discussed in Section 3. Some emerging security issues for multimedia information management systems will be discussed in Section 4. The topics to be discussed include secure digital libraries and secure semantic web. Privacy for multimedia information systems especially the problems that arise due to multimedia data mining will be discussed in Section 5. Summary and directions will be given in Section 6.

2 Multimedia database management systems

A multimedia data management system must provide the support for managing text, video, audio and image data. In addition, it must also manage multimedia data types. A multimedia database management system (MM-DBMS) is essentially a database management system (DBMS) that manages the multimedia data. Therefore, all of the issues in designing a DBMS apply for an MM-DBMS. That is, we need architectures and data models for MM-DBMSs. An MM-DBMS must also manage functions such as query processing and transaction management. In our previous papers we have given details on MM-DBMS (see [25]). In this section we summarize the information.

Various architectures are being examined to design and develop an MM-DBMS. In one approach, the DBMS is used just to manage the metadata, and a multimedia file manager is used to manage the multimedia data. Then there is a module for integrating the DBMS and the multimedia file manager. This architecture is based on the loose-coupling approach and consists of the three modules: the DBMS managing the metadata, the multimedia file manager, and the module for integrating the two. The second architecture is the tight coupling approach. In this architecture, the DBMS manages both the multimedia database as well as the metadata. That is, the DBMS is an MM-DBMS. The tight coupling architecture has an advantage because all of the DBMS functions could be applied on the multimedia database. This includes query processing, transaction management, metadata management, storage management, and security and integrity management. Note that with the loose coupling approach, unless the file manager performs the DBMS functions, the DBMS only manages the metadata for the multimedia data.

There are also other aspects to architectures as discussed in [22]. For example, a multimedia database system could use a commercial database system such as an object-oriented database system to manage multimedia objects. However, relationships between objects and the representation of temporal relationships may involve extensions to the database management system. That is, a DBMS together with an extension layer provide complete support to manage multimedia data. In the alternative case, both the extensions and the database management functions are integrated so that there is one database management system to manage multimedia objects as well as the relationships between the objects. Multimedia databases could also be distributed. In this case, we assume that each MM-DBMS is augmented with a Multimedia Distributed Processor (MDP) as discussed in [22].

In representing multimedia data, several features have to be supported. First of all, there has to be a way to capture the complex data types and all the relationships between the data. Various temporal constructs such as play-before, play-after, play-together, etc., have to be captured (see, for example, the discussion in [14]). An appropriate data model is critical to represent an MM-DBMS. Relational, object-oriented, as well as object-relational data models have been examined to represent multimedia data (see also [2, 33]). Some argue that relational models are better since they can capture relationships, while others argue that object models are better as they represent complex structures.

Languages such as SQL are being extended for MM-DBMS (see, for example, [18]). It appears that both relational and object models have to be extended to capture the temporal constructs and other special features. Associated with a data model is a query language. The language should support the constructs needed to manipulate the multimedia database. For example, one may need to query to play frames 500–1,000 of a video script. In summary, several efforts are under way to develop appropriate data models for MM-DBMSs. Standards are also being developed. This is an area that has matured within the past couple of years.

An MM-DBMS must support the basic DBMS functions. These include data manipulation, which includes query/update processing, transaction management, metadata management, storage management, and maintaining security and integrity. All of these functions are more complex since the data may be structured as well as unstructured. Furthermore, handling various data types such as audio and video is quite complex. In addition to these basic DBMS functions, an MM-DBMS must also support real-time processing to synchronize multimedia data types such as audio and video. Quality of service is an important aspect for MM-DBMS. For example, in certain cases, high quality resolution for images may not always be necessary. Special user interfaces are also needed to support different media.

Data manipulation involves various aspects. Support for querying, browsing, and filtering the data is essential. Appropriate query languages are needed for this purpose. As discussed earlier, SQL extensions show much promise. In addition to just querying the data, one also may want to edit the data. That is, two objects may be merged to form a third object. One could project an object to form a smaller object. As an example, objects may be merged based on time intervals, and an object may be projected based on time intervals. Objects may also be updated in whole or in part. Much of the focus on MM-DBMS has been on data representation and data manipulation. Various algorithms have been proposed. Some of these algorithms have also been implemented in various systems [17].

There has been some discussion as to whether transaction management is needed in MM-DBMS [15]. We feel this is important, as in many cases annotations may be associated with multimedia objects. For example, if one updates an image, then its annotation must also be updated. Therefore, the two operations have to be carried out as part of a transaction. Unlike data representation and data manipulation, transaction management in an MM-DBMS is still a new area. Associated with transaction management are concurrency control and recovery. The issue is what are the transaction models? Are there special concurrency control and recovery mechanisms? Much research is needed in this area.

Many of the metadata management issues for DBMSs also apply to MM-DBMSs. What is a model for metadata? What are the techniques for metadata management? In addition, there may be large quantities of metadata to describe, say, audio and video data. For example, in the case of video data, one may need to maintain information about the various frames. This information is usually stored in the metadata. There are several other considerations. Metadata plays a crucial role in pattern matching. To do data analysis on multimedia data, one needs to have some idea as to what one is searching for. For example, in a video clip, if various images are to be recognized, then there must be some patterns already stored to facilitate pattern matching. Information about these patterns has to be stored in the metadata. In summary, metadata management in an MM-DBMS is still a challenge. Some ideas were presented in [11]. The emergence of Internet technologies makes this even more complex.

The major issues in storage management include developing special index methods and access strategies for multimedia data types. Content-based data access is important for many multimedia applications. However, efficient techniques for content-based data access are still a challenge. Other storage issues include caching data. How often should the data be cached? Are there any special considerations for multimedia data? Are there special algorithms? Also, storage techniques for integrating different data types are needed. For example, a multimedia database may contain video, audio, and text databases instead of just one data type. The display of these different data types has to be synchronized. Appropriate storage mechanisms are needed so that there is continuous display of the data. Storage management for multimedia databases is also an area that has been given considerable attention. Several advances have been made during recent years [16].

Maintaining data integrity will include support for data quality, integrity constraint processing, concurrency control, and recovery for multi-user updates, and accuracy of the data on output. The issues on integrity for DBMSs are present for MM-DBMSs. However, enforcing integrity constraints remains a challenge. For example, what kinds of integrity constraints can be enforced on voice and video data? There is little research to address these issues. Security mechanisms include supporting access rights and authorization. There are also additional concerns. For example, in the case of video data, should access control rules be enforced on entire scripts or frames? We discuss security in detail in Section 3.

Other functions for an MM-DBMS include quality of service processing, real-time processing, and user interface management. For example, with respect to quality of service, in some instances one may need continuous display of data, and in some instances one could tolerate breaks of service. One has to come up with appropriate primitives to specify quality of service. Real-time processing plays a major role since appropriate scheduling techniques are needed to display various types of media such as voice together with video data. Finally, appropriate multimodal interfaces are needed for inputting and displaying multimedia data.

Data mining has an impact on the functions of multimedia database systems (see [22]). For example, the query processing strategies have to be adapted to handle mining queries if a tight integration between the data miner and the database system is the approach taken. This will then have an impact on the storage strategies. Furthermore, the data model will also have an impact. At present, many of the mining tools work on relational databases. However, if object-relational databases are to be used for multimedia modeling, then data mining tools have to be developed to handle such databases.

Typically data mining models data as a collection of similar but independent entities. The goal of data mining is to search for patterns that are common to many of these entities. Multimedia is harder to fit into this framework. Pictures and video of different buildings have some similarity—each represents a view of a building—but without clear structure such as "these are pictures of the front of buildings" it is difficult to relate multimedia mining to traditional data mining. Multimedia generally gives a lot of data on each entity, but not the same data for each entity.

A second difference between multimedia mining and structured data mining is the sequence or time element. Multimedia often captures an entity changing over time. Video and audio are clearly ordered, and even text has little meaning without sequence. Time series mining analyzes the change to one or more values over time. Multimedia is more complex—as the sequence progresses, the concept being represented may change as well. This is obvious with video, where a camera may pan or objects in the scene may move. Text shows such movement as well—for example this paper has moved from discussing multimedia data management to multimedia data mining and will later discuss security. Understanding and representing such change in the mining process is necessary to mine multimedia data.

This section has provided a brief overview of architectures, data models, functions and mining for MM-DBMSs. Further details can be found in [22]. The purpose of this section is to provide some background so that we can discuss security issues. Security and privacy are discussed in Sections 3, 4 and 5.

3 Security for multimedia database management systems

3.1 Overview

The previous section provided an overview of multimedia database management systems. It is critical that multimedia database systems be secure for a variety of applications including Command and Control and Intelligence. Security includes confidentially where sensitive information about the individuals are protected, secrecy where individuals are only given access to the data that they are authorized to know, and integrity where unauthorized and malicious modifications to the data are prohibited. Much work has been carried out on security for database systems (see for example [9] and [23] for an overview of the developments). There is some research on security for multimedia databases (see [19]). In this paper we examine security issues for multimedia databases. We also examine privacy where sensitive data and information about individuals are extracted as a result of multimedia data mining.

In Section 3.2 we discuss the elements that constitute a security policy for multimedia databases. We examine access control models as well as multilevel security for multimedia databases. We also discuss security constraints. Security architectures for multimedia data are discussed in Section 3.3. Security architectures are essentially architectures that identify the security critical components. Secure data models will be the subject of Section 3.4. Then in Section 3.5 we examine various multimedia database functions and discuss the security impact on these functions. Managing multimedia data in a secure distributed environment is discussed in Section 3.6. The inference problem for multimedia data is discussed in Section 3.7. Security constraint processing is also elaborated in Section 3.7. Security constraints are constraints that assign security levels to the multimedia data. Integrity, real-time processing and fault tolerance are discussed within the context of security in Section 3.8. That is, we discuss dependable multimedia database management.

In our discussion of security for multimedia database systems we make many assumptions. For example, we assume that the components that support the data management system are secure. These include the communication subsystem and operating system as well as the middleware. Note that to have a completely secure multimedia information system we need secure multimedia database management systems, secure multimedia information management systems, secure networks, secure operating systems, secure middleware and secure applications. That is, we need end-to-end security. We need to ensure that each component of the integrated system is secure. In this paper we will focus only on securing the Multimedia Data Manager component of the integrated system.

3.2 Security policy

Security policy essentially specifies the application specific security rules and application independent security rules. Application independent security rules would be rules such as

- The combination of data from two video streams is always sensitive
- User operating at level L1 cannot read/view data from a text object, image object, audio object or video object classified at level L2 if L2 is a more sensitive level than L1.

The second rule above is usually enforced for multilevel security. In a multilevel secure database management system users cleared at different clearance levels access the data assigned different sensitivity levels so that the user only gets the data he or she can access. For example, a user at the Secret level can read all the data at the Secret level or below and a user at the unclassified level can only read the unclassified data. The access control model enforced for multilevel secure database systems is the Bell and La Padula model. In this model a user can read data at or below his level and he can update data at or above his level. Database security researchers have strengthened the second rule and most database systems enforce a rule where a user updates data at his level (see [9]).

Now the main question is how does the policy apply for multimedia data? We could have video cameras operating at different levels. Video cameras operating in the Middle East may be highly classified while video cameras in Europe may be less classified. Classified instruments will gather classified data while unclassified instruments will gather unclassified data. Furthermore video data may be in the form of streams. Therefore we need access control policies for data streams. Within each level, one could enforce application specific rules.

Application specific security rules include the following:

- Only law enforcement officials have authorization to examine video streams emanating from video camera A.
- Data from video streams A and B taken together are sensitive.
- All the data emanating from video cameras in Washington DC federal buildings are sensitive while the data emanating from video cameras in North Dakota federal buildings are not sensitive.

Essentially applications specific rules are specified using security constraints. We discuss security constraint processing in a later section. Note that in addition to video streams the discussion also applies for document sources, audiotapes and image data.

Another question is do the multimedia data collection instruments at different levels communicate with each other? Now, if the Bell and LaPadula policy is to be enforced, a classified instrument cannot send any data to an unclassified instrument. Data can move in the opposite direction. The multimedia network must ensure such communication.

A multimedia data collection instrument could also be multilevel. That is, an instrument could process data at different levels. Data could be text, video, audio and imagery. The multilevel data collector can then give data to the users at the appropriate level. For example, a multilevel video camera may give Secret video streams to an Intelligence officer, while it may give out only unclassified streams or images to a physician. One could also enforce role-based access control where users access data depending on their roles. A physician may have access to video/audio information about the spread of diseases while he may not have access to video/audio data about potential terrorists.

Granularity of access control is a challenge for multimedia. In the case of text one could grant access at the chapter level or even at the paragraph level. One could also classify the existence of certain chapters or sections. In the case of images, one could grant access depending on the content or at the pixel level. In the case of audio and video, one could grant access at the frame level. For example, John can read frames 1,000–2,000 while he can update frames 3,000–4,000. He has no access to any of the other frames.

Security policy integration is a major challenge. That is, each multimedia database may enforce it own security policy and have its own constraints. The challenge is to integrate the different policies especially in distributed and federated environments. For example, in the case of a federation, each federation of multimedia databases may have its own policy, which is derived from the security policies of the individual databases. The policies of the federations will have to be combined to get an integrated policy. Many of the ideas have been obtained from our earlier work on security for federated database systems (see [20]).

3.3 Secure system architectures for multimedia database systems

Various security architectures have been proposed for secure database systems (see [9], [28]). Security architectures are essentially system architectures that have been designed with security in mind. In this section we will examine four architectures for secure multimedia data management.

Consider architecture I which is the Integrity Lock architecture. In this architecture, there is a trusted agent that resides between the multimedia data collector and the multimedia data manager. Trusted agents are processes that carry out security critical functions. The trusted agent computes a cryptographic checksum for each multimedia object (e.g., paragraphs, images, audio frames, video frames etc.) depending on the security level of the data collector and the value of the data. The data object, the level and the checksum are stored in the multimedia database. When the data is retrieved, the trusted agent recomputed the checksum based on the data value and the level that are retrieved. If the newly computed checksum equals the checksum that is stored, then the trusted agent assumes that the data has not been tampered with. The idea here is to make the multimedia data manager untrusted. It will be very hard to trust the multimedia data manager as these data managers could reside at different sites. The main question is, can we afford to have a trusted agent for each multimedia data manager or do we have a trusted agent to manage say a collection of multimedia data collectors? We need to carry out a tradeoff study in determining how many trusted agents do we need. In a resource-constrained environment, we may have to employ fewer trusted agents.

Next architecture we discuss is the distributed architecture. Here we partition the data depending on the level. Here again there is a trusted agent that receives multimedia data and sends the data to the appropriate multimedia data manager. Classified data is sent to the classified multimedia data manager and the unclassified data is sent to the unclassified multimedia data manager. These data managers could be managing text, images, audio, video or a combination of the data types. If data has to be retrieved say by an Intelligence officer then the trusted agent retrieves the data from both the classified and unclassified data managers. If the data has to be retrieved by say a Physician then the data is retrieved from only the unclassified data manager. There is however an issue whether data could be covertly leaked from a Trojan horse operating at the classified level by inserting some values into the query. For example, the fact that there is a mission called Operation X could be classified. However a Trojan horse at the classified level could send the query to the unclassified multimedia manager to retrieve the video script for Operation X. Now, one could enforce security constraints by the trusted agent to detect such violations. That is, the trusted agent could enforce the security constraint that the fact that Operation X exists is classified and not send the query to the unclassified multimedia data manager. Another option is to replicate all the unclassified multimedia data at the classified level.

The third architecture is the operating system providing access control architecture. Here, while each multimedia data manager can handle multiple levels, there is an instance of a multimedia data manager operating at each level. The multimedia data are partitioned and access to the data are managed by the operating system. That is, the Unclassified multimedia data are stored in an Unclassified file while the Secret multimedia data are stored in a Secret file. Then the data is recombined during query and managed by the multimedia data manager operating at the user subject's level. Note that with this architecture the multimedia data manager is untrusted.

The final architecture is the trusted architecture. That is, while the first three architectures keep the multimedia data manager untrusted, in this architecture we trust a portion of the data manager that is controlling access to the multimedia data. We need to conduct an architecture analysis study and experimentation to determine which architecture is suited for secure multimedia data management.

3.4 Secure data models for multimedia database systems

Security has an impact on the data models for MM-DBMSs. In Section 2 we stated that relational, object as well as object-relational data models have been examined for MM-DBMSs. We need to examine security properties for these models.

There has been a lot of research on secure data models especially for relational and object-oriented data models. A survey is given in [9]. For example, what is the granularity of classification? In the case of relational models, do we classify or grant access to entire relations or can we grant access at the attribute, tuple and element level? In the case of object models, do we grant access to objects and classes or can we grant access to parts of the objects? How do we classify a composite object? For example, can we grant access to certain paragraphs of documents and deny access to certain other paragraphs? Little work has been reported on secure object relational data models. These models will combine security properties for both relational and object data models. We need to revisit this research again for secure multimedia database system.

3.5 Security impact on multimedia data and information management functions

Security has an impact on all of the functions of a multimedia data manager. Consider the query operation. The query processor has to examine the access control rules and security constraints and modify the query accordingly. For example, if the fact that the existence of Operation X is classified, then this query cannot be sent to an unclassified multimedia data collector such as a video camera to film the event. Similarly the update processor also examines the access control rules and computes the level of the multimedia data to be inserted or modified. Security also has an impact on multimedia editing and browsing. When one is browsing multimedia data, the system must ensure that the user has the proper access to browse the link or access the data associated with the link. In the case of multimedia editing, when objects at different levels are combined to form a film, then the film object has to be classified accordingly. One may need to classify the various frames or assign the high water mark associated with the levels of the individual objects that compose the film. Furthermore, when films are edited such as certain portions are deleted, and then one needs to recompute the level of the object.

Secure multimedia transaction processing is another issue. First, what does transaction-processing mean? One could imagine data being gathered from two different locations (e.g. video streams) and make simultaneous updates to the multimedia database. Both updates have to be carried out as a transaction. This is conceivable if say an analyst needs both films to carry out the analysis. So assuming that the notion of a transaction is valid, what does it mean to process transactions securely? There has been a lot of work on secure transaction processing both for single level and multi-level transactions. In the case of a single level transaction it is assumed that the transaction is processed at a single security level. In the case of multilevel transactions, the transaction may operate at multiple security levels. The main challenge is to ensure that information does not flow covertly from a higher level to a lower level. Multimedia transaction processing will also have similar challenges. We need to examine the techniques from secure transaction processing and real-time transaction processing to see if we can develop techniques specific to dependable multimedia transaction processing.

Next consider the storage manager function. The storage manager has to ensure that access is controlled to the multimedia database. Storage manager may also be responsible for partitioning the data according to the security levels. The security impact of access methods and indexing strategy for multimedia data are yet to be determined. Numerous index strategies have been developed for multimedia data including for text, images, audio and video. We need to examine the strategies and determine the security impact.

Metadata management is also another issue. For example, we need to first determine the types of metadata for multimedia data. Metadata may include descriptions about the data, the source of the data as well as the quality of the data. Metadata may also include information such as Frames 100–2,000 are about president's speech. Metadata may also be classified. In some cases the metadata may be classified at a higher level than the data itself. For example, the location of the data may be highly sensitive while the data could be unclassified. We should, also ensure that one cannot obtain unauthorized information from the metadata.

3.6 Secure distributed multimedia data management

As we have stated in this paper, there may be multiple multimedia databases connected throughout the network. Some of the databases may contain single media data such as text; images, video or audio and some others may contain multimedia data. Some of them may be unstructured while some other may be semi-structured. There is also a need to connect multimedia data with relational and structured data. The collection of multimedia databases functions like a distributed database management system. Therefore, ensuring security for such a network is in many ways like ensuring security for distributed database management systems.

The distributed architecture we have discussed in the previous section is one such architecture that could be employed for a secure distributed multimedia data manager. That is, data is partitioned according to security levels and managed by a trusted agent. We may also want to connect several multimedia data managers each based on one of the architectures we have discussed in the previous section. That is, we can build a true secure distributed multimedia data manger by connecting the different secure multimedia data managers. We assume that the multimedia communication network that connects the multimedia data managers is secure. We have to ensure that when the different multimedia data managers are connected no higher-level information is sent to a lower level multimedia data manager. That is, we could assume that at each site there could be an instance of a multimedia data manager operating at level L communicating with another multimedia data manager also operating at level L.

Another challenge is to enforce distributed access control. Each multimedia node would have its own security policy. We need to form an integrated policy. The integrated policy has to be enforced across all the multimedia nodes. The aggregation problem is exacerbated as the multimedia data managers process data and the processed data may have to be aggregated across the data managers. The aggregated data may be highly sensitive. We discuss the inference problem in the next section.

3.7 Inference problem

Inference is the process of users or subjects deducing information from the legitimate responses received. If the deduced information is something that the user is not allowed to see then it becomes a problem. This is known as the inference problem. Various approaches have been proposed to handle the inference problem (see for example, [32]). One of the promising approaches to the inference problem is security constraint processing where some constraints are processed during database design where the data schemas are partitioned according to the security levels. Some constraints are processed during database updates and the data is assigned appropriate levels. Some constraints are processed during the query operation and the data is prevented from being released to the user. Some examples of security constraints were given in Section 3.2. These are application specific constraints.

In a shared data processing environment, because a lot of data has to be aggregated, there could be a potential for inference problems. That is, the aggregated data from multimedia nodes A, B and C could be highly sensitive. For example, one multimedia data manager could be managing video streams emanating from the situation in the Middle East and another multimedia data manager could manage video streams emanating from the situation in Asia and the combined sensed information could be highly sensitive. The inference controller has to examine the constraints and prevent such sensitive information from being released to individuals who are not authorized to acquire this information.

While much progress has been made on the inference problem for relational databases, we need to examine the techniques for multimedia databases. However new technologies such as data mining exacerbates the inference problem. That is, because with data mining, users now have tools to make all kinds of inferences some of which may be unauthorized. However we need data mining tools as they solve many security problems such as intrusion detection and auditing. Therefore, we need to develop data mining techniques that will control, some of the unauthorized inferences. We will revisit this topic under privacy in Section 5.

3.8 Quality of service for multimedia data management systems

Another challenge for multimedia data management is how do you make tradeoffs between security, integrity, fault tolerance and real-time processing. In many cases the data will have to satisfy integrity constraints. However security and integrity have some conflicts. For example, if Unclassified multimedia data managers may be managing say video streams of some events and the data gathered from the Secret multimedia data managers are not sent to the Unclassified managers for security reasons, the Unclassified managers are reasoning with incomplete information and one cannot have confidence on the results of the analysis. The question is what is more important: security or integrity? In a critical situation when there is just an unclassified data manager say managing video streams emanating from North Dakota and some action has to be taken immediately, then it may need some classified information to make the decision. However this will be a gross security violation. Therefore we need flexible techniques to have both integrity and security.

Another challenge is the conflict between security and real-time processing. If a multimedia data manager monitors the environment and must update the images within 5 s and if there are many access control checks as to whether the multimedia data manager can indeed update the data, then the timing constraint may be missed. Therefore, we need flexible techniques for ensuring security as well as real-time processing.

Fault tolerance is a major area for multimedia data management. For example, we cannot guarantee that all the multimedia data managers in different locations will be up all the time. The challenges include, backing up the data managers, replicating the data mangers, data managers rejoining networks with little disruption, utilizing the techniques developed for distributed data management with respect to commit protocols and distributed concurrency control algorithms for sensors, and ensuring that the data managers recover from faults in a secure environment. What we need is a quality of service manager to make tradeoffs between security, integrity real-time processing and fault tolerance. Finally there has been lot of work on using real-time techniques for presentation and synchronization of multimedia data (see [22]). We need to incorporate security into this research. For a discussion of integrating security and real-time processing for command and control systems we refer to [31].

4 Security issues for multimedia information management systems

4.1 Overview

Information management systems include database systems as well as digital libraries, information retrieval systems and data mining systems. Multimedia information management is having a major impact in several technologies including digital libraries, e-commerce, semantic web, document publishing and information retrieval, and stream processing especially for multimedia data. In addition there are also other technologies such as collaboration and knowledge management that need multimedia information management. For many of these applications the multimedia information management systems have to be secure. In this section we will discuss some of the security issues.

The organization of this section is as follows. In Section 4.2 we discuss security for digital libraries. Multimedia information management for secure e-commerce will be discussed in Section 4.3. Security for semantic web, which involves managing multimedia data, will be the subject of Section 4.4. Secure publishing of multimedia documents will be discussed in Section 4.5. Secure stream information management will be discussed in Section 4.6. Multimedia for secure collaboration and knowledge management will be discussed in Section 4.7.

4.2 Secure digital libraries

Digital libraries are essentially about storing, processing, managing and analyzing collections of digitized documents. These documents could contain text, images, audio and video data. One can envisage digital libraries to be hypermedia information systems, which are essentially multimedia information objects that are linked. That is, one can browse the multimedia documents by traversing the links.

All of the security challenges discussed for multimedia databases such as secure query processing, secure storage and managing metadata securely are challenges for digital libraries. In addition, we need to be concerned about copyright protection, protecting the links and nodes while browsing the documents as well as special security models for the digital libraries. There has been some research on secure digital libraries (see for example [9]). There is still much to be done.

4.3 E-commerce security

Multimedia plays an important role for e-commerce. This area is now called multimedia-commerce or M-Commence. While carrying out e-commerce, various documents have to be interchanges. Much of the information such as contracts, billing data and other transaction data may contain text as well as other media. There has been some on secure e-commerce (see [12]). We also need to examine security for m-commerce.

For example, XML is being used to represent many of the documents. Extensions to XML such as SMIL (Synchronized Multimedia Language) have been proposed for representing multimedia documents. We need to ensure that that these documents are accessed only by authorized individuals. There has been some work on XML security (see [4]). We need to examine security for multimedia documents on the web.

4.4 Secure semantic web

Tim Berners Lee has specified various layers for the semantic web (see [3]). At the lowest level one has the protocols for communication including TCP/IP (Transmission Control Protocol/Internet protocol), HTTP (Hypertext Transfer Protocol) and SSL (Secure Socket Layer). The next level is the XML layer that also includes XML schemas. The next level is the RDF layer. Next come the Ontologies and Interoperability layer. Finally at the highest-level one has the Trust Management layer.

The challenge is, how can we trust the information that the web gives us? Closely related to trust is security. However security cannot be considered in isolation. That is, there is no one layer that should focus on security. Security cuts across all layers and this is a challenge. For example, consider the lowest layer. One needs secure TCP/IP, secure sockets, and secure HTTP. There are now security protocols for these various lower layer protocols. One needs end-to-end security. That is, one cannot just have secure TCP/IP built on untrusted communication layers. That is, we need network security. Next layer is XML and XML schemas. One needs secure XML. That is, access must be controlled to various portions of the document for reading, browsing and modifications. There is research on securing XML and XML schemas. The next step is securing RDF. Now with RDF not only do we need secure XML, we also need security for the interpretations and semantics. For example under certain context, portions of the document may be Unclassified while under certain other context the document may be Classified. As an example one could declassify an RDF document, once the war is over. Lot of work has been carried out security constraints processing for relational databases. One needs to determine whether these results could be applied for the semantic web (see [5, 30]).

Once XML and RDF have been secured the next step is to examine security for ontologies and interoperation. That is, ontologies may have security levels attached to them. Certain parts of the ontologies could be Secret while certain other parts may be Unclassified. The challenge is how does one use these ontologies for secure information integration? Researchers have done some work on the secure interoperability of databases. We need to revisit this research and then determine what else needs to be done so that the information on the web can be managed, integrated and exchanged securely.

4.5 Secure publishing of multimedia documents

Whether it is for digital libraries or for semantic web or for m-commerce, we may need to publish multimedia documents on the web. Security is an important consideration for publishing documents. In [4] some interesting work was reported on secure publishing of XML documents. The idea is for owners to specify access control policies on users and third party publishers to enforce the access control policies when disseminating the documents. Now, if the third party is trusted then no additional work is necessary. However it is almost impossible to trust all of the agents on the web. Therefore the challenge is to use appropriate encryption techniques and ensure that the user only gets the documents he is authorized to get.

We need to examine such work for publishing multimedia documents on the web. Publishing XML documents is just the first step. As we have stated, extensions to XML have been proposed for representing multimedia documents. The challenge is how do you publish text, image, audio and video documents securely on the web in the midst of untrusted third parties? We need more research to address these challenges.

4.6 Secure stream information processing

Stream information management has received much attention (see [7]). However little work has been reported on security issues. Stream data is continuous data emanating say from sensors and network devices. Often the data is transient. Stream data management issues include developing appropriate query processing and storage strategies.

Security issues for stream information processing were briefly examined in [29] as part of security for sensor databases. For example, what type of access control can you enforced on streams. What happens when data is aggregated? Another challenge is what happens when malicious programs corrupt the data? For example, some results on computing correct aggregate results from possibly corrupted individual data sources were examined in [13]. There is still lot more research to be done in this area. Inference problem when aggregating streams is also an issue.

4.7 Other security issues

The previous sections focused on security for semantic web, digital libraries, stream information management, and e-commerce with respect to managing multimedia data.

There are several other security challenges. For example, multiple users may collaborate with each other and may exchange multimedia documents. We need to investigate security issues for multimedia documents used for collaboration.

Secure knowledge management is also another challenge for multimedia information management. For example, how do we protect the intellectual property of an organization? The intellectual property may be in the form of video/audio recordings, documents and presentations with animations. How do you securely store and manage this information? Secure knowledge management challenges also include managing multimedia documents on corporate Intranets. There is still a lot of research to be done in this area.

5 Privacy considerations

5.1 Overview

Privacy is about protecting information about individuals. Privacy has been discussed a great deal in the past especially when it relates to protecting medical information about patients. Social scientists as well as technologists have been working on privacy issues. However, privacy has received enormous attention during the past year. This is mainly because of counter-terrorism and national security. For example in order to extract information about various individuals and perhaps prevent and/or detect potential terrorist attacks data mining tools are being examined. We have heard a lot about national security vs. privacy in the media. This is mainly due to the fact that people are now realizing that to handle terrorism, the government may need to collect data about individuals and mine the data to extract information. Data may be relational or it may be text, video and images. This is causing a major concern with various civil liberties unions (see [24, 27]).

In this section we discuss privacy threats that arise due to data mining and multimedia data mining. We also discuss some solutions. Section 5.2 will discuss issues on multimedia data mining, national security and privacy. Some potential solutions are discussed in Section 5.3.

5.2 Multimedia data mining, national security and privacy

With the world wide web, there is now an abundance of data information about individuals that one can obtain within seconds. The data could be structured data or could be multimedia data such as text, images, video and audio. Information could be obtained through mining or just from information retrieval. Therefore, one needs to enforce controls on databases including multimedia databases and data mining and multimedia data mining tools. This is a very difficult problem especially with respect to multimedia data mining. In summary, one needs to develop techniques to prevent users from mining and extracting information from the multimedia data whether they are on the web or on servers. Now this goes against all that we have said about data mining in our previous papers (see for example, [21]). That is, we have portrayed data mining as a technology that is critical for say analysts and other users so that they can get the right information at the right time. Furthermore, they can also extract patterns previously unknown. This is all true. However, we do not want the information to be used in an incorrect manner. For example, based on information about a person, an insurance company could deny insurance or a loan agency could deny loans. In many cases these denials may not be legitimate. Therefore, information providers have to be very careful in what they release. Also, data mining and multimedia data mining researchers have to ensure that privacy aspects are addressed.

While little work has been reported on privacy issues for web and mining, we are moving in the right direction. As research initiatives are started in this area, we can expect some progress to be made. Note that there are also social and political aspects to consider. That is, technologists, sociologists, policy experts, counter-terrorism experts, and legal experts have to work together to develop appropriate data mining and multimedia data mining techniques as well as ensure privacy. Some potential solutions to the privacy problem that arise due to data mining are discussed in the next section.

5.3 Solutions to the privacy problem

As we have mentioned, the challenge is to provide solutions to enhance national security but at the same time ensure privacy. There is now research at various laboratories on privacy enhanced/sensitive data mining (e.g., Agrawal at IBM Almaden, Gehrke at Cornell University and Clifton at Purdue University, see for example [1, 6, 10]). The idea here is to continue with mining but at the same time ensure privacy as much as possible. For example, Clifton has proposed the use of the multiparty security policy approach for carrying out privacy sensitive data mining. While there is some progress we still have a long way to go. Some useful references are provided in [6] (see also [8]).

We give some more details on an approach we are proposing. Note that one mines the data and extracts patterns and trends. The privacy constraints determine which patterns are private and to what extent. For example, suppose one could extract the names and healthcare records. If we have a privacy constraint that states that names and healthcare records are private then this information is not released to the general public. If the information is semi-private, then it is released to those who have a need to know. Essentially the inference controller approach we have discussed is one solution to achieving some level of privacy. It could be regarded to be a type of privacy sensitive data mining. In our research we have found many challenges to the inference controller approach we have proposed (see [30]). These challenges will have to be addressed when handling privacy constraints (see also [26]).

Much of the work on privacy preserving data mining focuses on relational data. We need to carry out research on privacy preserving multimedia data mining. There have been some discussions on privacy preserving text data mining. We need to combine techniques for privacy preserving data mining with techniques for multimedia data mining to obtain solutions for privacy preserving multimedia data mining.

6 Summary and directions

This paper has provided some of the developments and directions in secure multimedia database management. We started with a discussion of multimedia data management and mining and then focused on security issues. Then we discussed privacy concerns.

There is still a lot to be done. Security research for multimedia database management is just beginning. While there have been some efforts over the past decade, there is still much to be done on developing security policies, architectures and query strategies. Privacy issues are even more challenging. We are only beginning research in multimedia data mining and privacy preserving data mining. Therefore we have a long way to go before we develop practical solutions for privacy preserving multimedia data mining. We have provided some initial directions in this paper.

Acknowledgement I thank NSF and the MITRE Corporation for their support to continue my work on data mining, counter-terrorism, information security and privacy.

Disclaimer The views and conclusions expressed in this paper are those of the author and do not reflect the policies or procedures of the National Science Foundation, the MITRE Corporation or of the US Government.

References

1. Agrawal R, Srikant R (2000) Privacy-preserving data mining. In: Proceedings of the ACM SIGMOD Conference, Dallas, TX, May
2. Banerjee J et al (1987) A data model for object-oriented applications. ACM Trans Off Inf Sys, pp. 3–26, April
3. Berners Lee T et al The semantic web. Sci Am, pp. 28–37, May
4. Bertino E, Ferrari E, Squicciarini AC (2003) X-TNL: An XML-based language for trust negotiations. Proceedings of the IEEE POLICY Workshop, Lake Como, Italy
5. Bertino E et al (2004) Secure third party publishing of XML documents. IEEE Trans Knowl Data Eng, pp. 1263–1278, October
6. Clifton C et al (2002) Defining privacy for data mining. In: Next Generation Data Mining Workshop, Baltimore, MD, November
7. Dobra A et al (2002) Processing complex aggregate queries over data streams. In: Proceedings of the 2002 ACM Sigmod international conference on management of data, Madison, WI, June
8. Evfimievski A et al (2002) Privacy preserving mining of association rules. In: Proceedings of the eighth ACM SIGKDD international conference on knowledge discovery and data mining. Edmonton, Alberta, Canada, July
9. Ferrari E, Thuraisingham B (2000) Database security, Artech House, October (editors: M. Piattini and O. Diaz), pp. 160–180
10. Gehrke J (2002) Research problems in data stream processing and privacy-preserving data mining. In: Proceedings of the next generation data mining workshop, Baltimore, MD, November
11. Thuraisingham N (ed) (1996) Proceedings of the 1st IEEE Metadata Conference. Silver Spring, MD, April
12. Ghosh A (1998) E-Commerce Security: weak links, best defenses. John Wiley, Mississauga, Ontario, Cananda
13. Perrig A et al (2003) SIA: secure information aggregation in sensor networks. Technical report, Carnegie Melon University, April
14. Prabhakaran B (1997) Multimedia database systems. Kluwer, MA, June
15. Berra B, Nowsu K, Thuraisingham B (eds) (1994) Proceedings of the ACM multimedia conference workshop on multimedia database management systems, San Francisco, CA, October 1994
16. Bayard H, Lavander B, Kerchner M, Thuraisingham B, Zemankova M (eds) (1994) Proceedings of the massive digital data systems workshop. Community Management Staff, Washington D.C., February 1994
17. Ghafoor A, Little T (eds) (1993) Special issue on multimedia database systems. IEEE Trans Knowl Data Eng, April 1993
18. SQL3 (1992) American National Standards Institute, Draft, December
19. Thuraisingham B (1990) Multilevel security for multimedia database systems. In: Proceedings of the IFIP database security conference, Halifax, UK, September
20. Thuraisingham B (1994) Security issues for federated database management. Computers and Security, December
21. Thuraisingham B (1998) Data mining: technologies, techniques, tools and trends. CRC, December
22. Thuraisingham B (2001) Managing and mining multimedia databases. CRC, June
23. Thuraisingham B (2002) Data and applications security: developments and directions. In: Proceedings of the IEEE COMPSAC conference, Oxford, UK, August
24. Thuraisingham B (2003) Data mining, national security, privacy and civil liberties, SIGKDD Explorations, January

25. Thuraisingham B (2003) Management and mining multimedia databases. International Journal of Tools in Artificial Intelligence, volume 13, September 2004, pp. 730–749
26. Thuraisingham B (2003) Privacy constraints processing in a privacy enhanced database management system. Data Knowl Eng (in press)
27. Thuraisingham B (2003) Web data mining technologies and their applications to business intelligence and counter-terrorism. CRC, June
28. Thuraisingham B (2004) Database and applications security: integrating data management and applications security. CRC, December
29. Thuraisingham B (2005) Secure sensor information management. IEEE Signal Process Mag, pp. 14–19, May
30. Thuraisingham B, Ford W (1995) Security constraint processing in a distributed database management system. IEEE Trans Knowl Data Eng, pp. 274–293, April
31. Thuraisingham B, Maurer J (1999) Survivability of real-time command and control systems. IEEE Trans Knowl Data Eng, pp. 228–238, January
32. Thuraisingham B et al (1993) Design and implementation of a database inference controller. Data Knowl Eng, pp. 271–288, December
33. Woelk D et al (1986) An object-oriented approach to multimedia databases. In: Proceedings of the ACM SIGMOD conference, Washington DC, June

Dr. Bhavani Thuraisingham is the Program Director for Cyber Trust and Data and Applications Security at the National Science Foundation and has been on IPA to NSF from the MITRE Corporation since October 2001. She is part of a team at NSF setting directions for cyber security and data mining for counter-terrorism. She has been with MITRE since January 1989 where was the department head in Data and Information Management in the Information Technology Division and later chief scientist in data management in MITRE’s Information Technology Directorate. She has conducted research in secure databases for over 18 years and is the recipient of IEEE Computer Society’s 1997 Technical Achievement Award and recently IEEE’s 2003 Fellow Award for her work in database security. She is also a 2003 Fellow of the American Association for the Advancement of Science. Dr. Thuraisingham has published over 200 refereed conference papers and over 60 journal articles in secure data management and information technology. She serves (or has served) on editorial boards of journals including IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Dependable and Secure Computing, ACM Transactions on Information and Systems Security, the Journal of Computer Security and Computer Standards and Interface Journal. She is the inventor of three patents for MITRE on Database Inference Control and has written six books on data management and data mining for technical managers and is currently writing a text book on database and application security based on her work the past 18 years. Her research interests are in secure semantic web, sensor information security, and data mining for count-terrorism.