International Journal of Computer Science and Software Engineering (IJCSSE), Volume 4, Issue 7, July 2015
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 172-177

Multimedia System Security Using Access Control Policy Based on Role Based Access Control

Roslina[1], Hartono[2] and Muhammad Zarlis[3]

[1] Politeknik Negeri Medan., Department of Computer Science, University of Sumatera Utara, Medan, 20155

[2, 3] Department of Computer Science, University of Sumatera Utara, Medan, 20155

[1]roslinanich@gmail.com, [2]hartonoibbi@gmail.com, [3]m.zarlis@usu.ac.id

ABSTRACT

Multimedia data and information systems manage, communicate, and present multimedia data including text, images, audio and video. We need to ensure that the data is protected from unauthorized access as well as malicious corruption. Digital watermarking techniques that insert hidden copyright messages into the multimedia data are needed. Furthermore, since multimedia data is being used for security applications such as surveillance and monitoring, protecting privacy of the individual is crucial. This paper will discuss the security of multimedia systems using access control policies. An access control space represents the permission assignment state of a subject or role. Nowadays, three kinds of access control, discretionary access control (DAC) mandatory access control (MAC) and role-based access control (RBAC) have been proposed. In RBAC, there are role hierarchies in which a senior role can perform the permission of a junior role. Role Based Access Control (RBAC) is a popular model for access control policy and is used widely as it provides a convenient way to specify entitlements corresponding to specific meaning. One of the biggest issue in RBAC is authentication is for ensuring secure exchange of information and preventing illegal modification. In this paper, the description of an access control algorithm and a system architecture for a secure multimedia system are presented and also the method for securing information exchange in multimedia system.

Keywords: *Access Control, Role Based Access Control (RBAC), Multimedia System.*

1. INTRODUCTION

Multimedia data and information systems manage, communicate, and present 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. 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 [11]. 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. For this meaning we can use an access control [4]. An access control space represents the permission assignment state of a subject or role [5]. According to Na and Cheon [7], Nowadays, three kinds of access control, discretionary access control (DAC) mandatory access control (MAC) and role-based access control (RBAC) have been proposed. In RBAC, there are role hierarchies in which a senior role can perform the permission of a junior role. RBAC determines access permissions that roles can perform, and assigns roles to users. Users can access objects according to assigned roles to them. As a result, the organization can not only preserve access control policy appropriate to its characteristics consistently, but also maintain access control relationship between subjects and objects independently [1].

2. MULTIMEDIA DATABASE MANAGEMENT SYSTEM

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 [8]. 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 [12]. Using An Access Control, we can divide the user according to their content-based data access. 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, 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. From this point, we also can use this access control to manage the user that can access the multimedia database management system [9].

2.1 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 :

a. The combination of data from two video streams is always sensitive.

b. 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.

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.
Application specific security rules include the following:

a. Only law enforcement officials have authorization to examine video streams emanating from video camera A.

b. Data from video streams A and B taken together are sensitive.

c. 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.

2.2 Access Control in Multimedia Database Management System

According to Thuraisingham [10]. 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 [10].

3. ACCESS CONTROL

Access control is the problem of determining the operations (e.g., read and write) that subjects (e.g., users and services) can perform on objects (e.g., files and network connections). A particular access control specification instance (or policy) is called a configuration. The addition of a safety specification greatly complicates an access control policy for three reasons: (1) constraint expressions are more complex than access control expressions, in general; (2) constraint expressions are not fail-safe; and (3) constraints can introduce conflicts with the access rights specification [5].

Nowadays, three kinds of access control, discretionary access control (DAC) mandatory access
control (MAC) and role-based access control (RBAC) have been proposed. MAC enforces access controls on the basis of information security labels attached to users and objects. It shows access control
relationship that cannot be changed by the object's owner. MAC can determine all kinds of access controls between subjects and objects consistently. If some object is duplicated, access control relationship to the original object must be equally applicable to the duplicated object. Also the object's owner cannot change access control relationship. Security labels have to be granted to all subjects and objects by the system supervisor, and it can be changed only in accordance with the contents of the object [7].
In case of DAC, access control restricts the access to the object on the basis of the identity of the user or the group. The owner of the object determines access control relationship. Therefore, it is difficult to maintain access control consistency. Access control
can be established in one subject-object unit, and users who have permissions can allow any other users to access to data. But, because access control policy can be changed at the owner's own discretion, and owners can optionally delegate their authorities to other subjects, it is difficult to control information efficiently. Information related to the meaning of data cannot be involved in DAC, because access control is only based on qualifications of subjects [2].
Compared with MAC and DAC, RBAC determines access permissions that roles can perform, and assigns roles to users. Users can access objects according to assigned roles to them. As a result, the organization can not only preserve access control policy appropriate to its characteristics consistently, but also maintain access control relationship between subjects and objects independently. Even if access control policy is changed, the new access rights have to be allowed not to the user but to the role itself. RBAC can manage the complicated security policy efficiently [1].

4. ROLE BASED ACCESS CONTROL

A role in RBAC is the aggregate of responsibility and authority, to which the access to the object is permitted [5]. Each role having relations with other roles exists in role hierarchies according to the access control policy. Senior roles inherit authorities of junior role [9]. In this case, the outstanding problem is that a junior role or the role, which is not included in hierarchies, cannot perform permissions of a senior role.

In RBAC, it is possible to simplify the complicated form of an organization's access control
policy. Access decisions are based on the roles, which is part of an organization. RBAC is a non-discretionary access control in which the system administrator allows the role's permissions to the user by defining user, role, and permission. The system administrator divides roles according to operations in an organization, and gives access permissions to roles. The administrator of the system or organization gives access permissions to roles, and users are endowed with roles according to their responsibility and obligation [7].

4.1 Role Based Access Control Components

According to Na and Cheon[7], The basic components of RBAC model are User, Role and Permission. User is a person, who uses the system or an application program within the system. Membership to roles is granted to users based on their obligation and responsibility in the organization. The operation of a user can be carried out based on the user's role. Role means a set of functional responsibilities within the organization. The system administrator defines roles, a combination of obligation and authority in organization, and assigns them to users. User-Role relationship represents collection of the user and role (Na). Fig. 1 presents the Basic Model of RBAC.

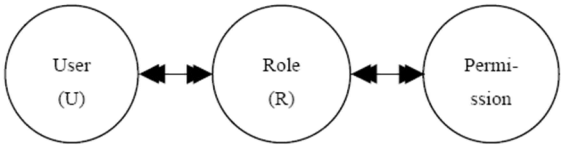

Fig. 1. Basic Model of RBAC [7]

4.2 Role-Permission (R-P) Relationship

Permission consists of obligation and authorization [5]. The former is the aggregate of operations that the pertinent role must perform or not, and the latter is the collection of operations that are permitted to roles or not. Expressions of obligation and authorization are simplified as defined in [7].

{identifier, mode, role, {action}, target, constraints, exception}

[identifier] : Uniquely identifying the permission
[mode] : o:obligation, a:authorization +:positive,-:negative
[role] : role which can process this permission
[action] : actual operation by permission
[target] : object which operation being applied
[constraints] : limit the applicability of the permission
[exception] : exceptional condition

Identifier is used to identify the permission. Mode specifies obligation and authorization, with either + and - denoting a positive or a negative policy respectively. e.g. o+ denotes a positive obligation. Role is to carry out this permission. Action means operation, which is to be processed by role, target is
object influenced by action in permission. Constraints represent limits the applicability of the permission, e.g. a time period, or execution condition. Exception represents exceptional condition for permissions to be executed or not, e.g. if a permission has a mode then this permission is not executed by the indicated role, but some specified exceptional condition occurred then permission can be allowed to be executed by the role. For instance, obligation such as "a nurse must check the patient's condition every morning at 8 o'clock" can be expressed as {np1, o+, nurse, {Check}, patient, every 08:00, -}. And authorization such as "a specialist can read chart of patient by intern" can be changed as {dp1, a+, specialist, {read}, chart by intern, -, -} [7].
The example of Role-Permission relationship used in this paper is presented in Table 1.

Table 1: Simplified Role-Permission Relationship Model

Role Group	Permission
Doctor	{dp1, a+, specialist,{read,fix},chart by intern, -, -}
	{dp2, o+, specialist,{chief of surgical operation}, patient, -,-}
	{dp3, a+, resident,{support of surgical operation}, specialist, request of specialist,-}
	{dp4, a-, resident,{read,fix}, chart by intern, -, no specialist}
	{dp5, a+, intern,{make}, chart for patient, -, -}
	{dp6, o-, intern,{chief of sugical operation}, patient, -, -}
Nurse	{np1, o+, chief nurse,{assign}, nurse-patient,every 09:00, -}
	{np2, a+, nurse,{injection by chart}, patient, by chart,-}
	{np3, a-, nurse,{preparation of medicine},drug,-,emergency}
Pharmacist	{pmp1, a+, pharmacist, {preparation of medicine}, patient by chart, doctor request, -}
	{pmp2, o+, pharmacist, {make report}, used drug, every 18:00, -}

Role Group and Group Relation Model can be seen in Figure 2.

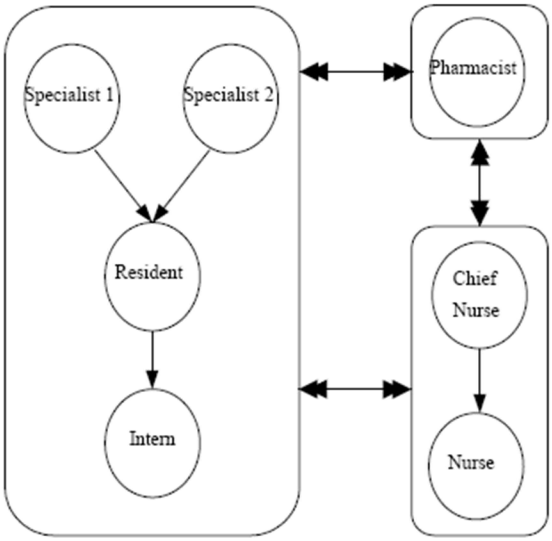

Fig. 2. Role Group and Group Relation Model [7]

4.3 Application

Usage-based RBAC models define a conservative security policy since users are assigned only those permissions which they actually use and this reduces operational risk. Generative models also model exactly how users actually use the permissions. For instance generative models will distinguish the role of a backup to an administrator who has the same entitlements but only uses them occasionally. Besides these directly apparent benefits, generative role models have many interesting applications which we are investigating in ongoing work.

a. Policy Reconciliation: Generative models can be used to reconcile with traditional RBAC models built from entitlements. This yields useful insights such as the evolution of role definitions when users begin to use some permissions more than others.

b. Identifying Policy Errors: Generative models can be used to identify a number of errors in policies such as overprovisioned users as well as users who have different attributes than other users using the same permisions.

c. Anomaly Detection: By comparing generative models across different periods of time, one can deduce changes in user behavior in terms of permission usage. This could flag anomalous behavior such as user who starts using an entirely new set of permissions (Molloy et.al).

4.4 Critical Issue in RBAC

The RBAC methods can be used for access control policy and is used widely as it provides a convenient way to specify entitlements corresponding to specific meaning. The problem occured when the information in multimedia system has been exchange from one person to another person. Authentication is protectiong the content integrity of digital document and secure data sharing. In this paper we propose, one of the method can be used in RBAC for ensuring the authentication is using fragile watermarking.
Fragile watermarking [13] is an important technique in the field of image authentication. It is used to protect the integrity of valuable images. In general, the available fragile watermarking approaches embed an authentication code into the protected image. The authentication code can be a logo, a trademark, or other copyright information. Then, the authentication code can be extracted to authenticate the image content. If parts of the authentication data are lost, the fragile watermarking scheme will be able to detect and indicate the tampered areas.
According to the embedding manner, the fragile watermarking technique can be classified into two
types: block-wise and pixel-wise. In the block-wise approach, the protected image is divided into several blocks. An authentication stream which derived from the hash result of block content is then embedded into the block itself. By comparing the extracted authentication stream with the hash result from the new block, the verifier can identify the integrity of the block. Normally, the block-wise approach is capable of detecting a considerable tampered area and improving the security protection [13].
Nevertheless, the detection ability of the block-wise fragile watermarking approach is insensitive and incapable of precisely identifying the tampered pixels. Moreover, the misjudgement problem occurs
frequently. Zhang and Wang [14] have proposed a pixel-wise fragile watermarking approach for detecting and locating the tampered pixels sensitively.

5. DISCUSSION

We also need a multimedia system to ensure that the data is protected from unauthorized access as well as malicious corruption. Now days, access control policy has been widely used as method for monitoring, protecting and ensuring the security and authentication of the information in multimedia system. Nowadays, three kinds of access control, discretionary access control (DAC) mandatory access control (MAC) and role-based access control (RBAC) have been proposed. In RBAC, there are role hierarchies in which a senior role can perform the permission of a junior role. Role Based Access Control (RBAC) is a popular model for access control policy and is used widely as it provides a convenient way to specify entitlements corresponding to specific meaning. The problem occured when the information in multimedia system has been exchange from one person to another person. Authentication is protectiong the content integrity of digital document and secure data sharing. One of the method that can be used in RBAC for ensuring the authentication is using fragile watermarking.

6. CONCLUSION

Security in Multimedia system today, are very important issue. This issue become more important for ensure that the data is protected from unauthorized access as well as malicious corruption. One of the method that can be used for securing the multimedia management database system is using access control. 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 using access control. Nowadays, three kinds of access control, discretionary access control (DAC) mandatory access control (MAC) and role-based access control (RBAC) have been proposed.
In RBAC, there are role hierarchies in which a senior role can perform the permission of a junior role. Role Based Access Control (RBAC) is a popular model for access control policy and is used widely as it provides a convenient way to specify entitlements corresponding to specific meaning.
Authentication is protectiong the content integrity of digital document and secure data sharing. One of the method that can be used in RBAC for ensuring the authentication is using fragile watermarking.

REFERENCES

[1] David F. Ferraiolo and Richard Kuhn. 1992. Role-based access control. Proceedings of the 15th NIST-NSA National computer security conference.--> Paper 6 in Na
[2] Department of Defense(USA), Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200-78-STD, DoD, 1985.--> Paper 2 in Na
[3] E. C. Lupu, M. S. Sloman. 1997. A Policy Based Role Object Model, Proceeding of IEEE EDOC'97.-->Paper 1 I Na
[4] Ferrari E, Thuraisingham B. 2000. Database security. Artech House, October (editors: M. Piattini and O.Diaz), pp. 160–180 paper 9 Thuraisingham
[5] Jaeger, Trent and Xiaolan Zhang. 2003. Policy Management Using Access Control Spaces. International Journal of ACM Transactions Vol. 6 No. 3: pp. 327-364
[6] Molloy, Ian, Park Youngja and Suresh Chari. Generative Models for Access Control Policies: Applications to Role

Mining Over Logs with Attribution. Proceedings of the 17th ACM symposium on Access Control Models and Technologies: pp. 45-56
[7] Na, SangYeob and Cheon, SuhHyun. 2000. Role Delegation in Role-Based Access Control. Proceedings of The Fifth ACM Workshop on Role-Based Access Control: pp. 39-44 Ketiga
[8] Prabhakaran B. 1997 Multimedia database systems. Kluwer, MA, June Paper 14 in Thuraisingham
[9] Ravi S. Sandhu, Edward J.Coyne, Hal L. Feinstein and Charles E. Youman. 1996. Role-Based Access Control Models. IEEE computer Vol. 29, number 2 : pp. 38 – 47 paper 7 in Na
[10] Thuraisingham B (1994) Security issues for federated database management. Computers and Security, December Paper 20 Thuraisingham
[11] Thuraisingham, Bhavani. 2007. Security and Privacy for Multimedia Database Management Systems. International Journal of Multimedia Tools Vol. 33 : pp. 13-29
[12] Zemankova M, Bayard H, Lavander B, Kerchner M, Thuraisingham B(eds). 1994. Community Management Staff. Proceedings of the massive digital data systems workshop.
[13] Lin, Pei Yu, Jung San Lee and Chin Chen Chang. 2011. Protecting the Content Integrity of Digital Imagery with Fidelity Preservation. Journal of ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM): 15: 1-20.
[14] Zhang, X. and Wang, S. 2009. Fragile watermarking scheme using hierarchical mechanism. Signal Process Vol. 89 No. 4: 675–679.

AUTHOR PROFILES:

Roslina received the Master degree in 1999 from National University of Malaysia (UKM) Malaysia in Information Technology and Bachelor Degree in 1994 from STMIK YPTK Padang, Indonesia in Computer Science. She is a lecturer at Politeknik Negeri Medan. Her current interests are in data mining and artificial intelligence. Nowadays, She Is a Student in a Doctoral Program in Computer Science at University of Sumatera Utara (USU). Research on Database, Data mining, Management Information Systems and Decision Support System.

Hartono received the Master degree in 2010 from the University of Putra Indonesia "YPTK" Padang, Indonesia in Computer Science and Bachelor Degree in 2008 from STMIK IBBI Medan, Indonesia in Computer Science. He is a lecturer at STMIK IBBI Medan. His current interests are in data mining and artificial intelligence. Nowadays, He Is a Student in a Doctoral Program in Computer Science at University of Sumatera Utara.

Muhammad Zarlis, He is a lecturer in a Doctoral Program in Computer Science at University of Sumatera Utara (USU).