A Secure Model for Distribute Multimedia Document, Based on Object Extraction of Data Content

Fatemeh Moradi
Computer Engineering and Information Technology
Payam Noor University
Tehran, Iran
fatmoradi@yahoo.com

Seyed Ali Razavi Ebrahimi
Computer Engineering and Information Technology
Payam Noor University
Tehran, Iran
dr_ali_razavi@yahoo.com

Ahmad Faraahi
Computer Engineering and Information Technology
Payam Noor University
Tehran, Iran
afaraahi@pnu.ac.ir

***Abstract*— Research in the field of security access in multimedia data is intended file structure, only as a single entity. In multimedia databases, metadata information and major objects extracted for indexing and searching purposes. Since the use of information access control and legitimate broadcast of sectors, are less discussed, in the proposed model, the necessity of deploying these objects to improve system security is investigated. This model is based on development of Web-Matrix model that provides extraction and access to multimedia objects. In this paper, we survey existing publisher multimedia object models, while we consider security techniques for media content. The security models assessment is possible with identifying and removing threats, protecting vulnerable resources and services, that modeling our proposed schema with KAOS method analyze security implementation of system, identify and estimate security critical requirements.**

***Keywords*— Multimedia Database, Web-Matrix Model, Object Extract, Multimedia Content Protection, KAOS Method.**

I. INTRODUCTION

The birth of Internet and development of computer network equipment provided instant access to data and information. With the development of information technology applications, data protection becomes a necessity [1].

Main security services include authentication, access control, authorization, data integrity, Non repudiation and availability [2]. These services should be implemented appropriately to reduce possible attacks on the data. Also it is possible to secure the data in file-level access, ensuring that only authorized entities can access multimedia files.

Although security was always a concern, however, the main concepts of security services, is limited to the computer system files. These services are considered file security entities to be a single structure. Only some specific systems, have presented access to parts of files based on user permissions [3], which is essential for further research will be done in the area of access control in content.

The model presented in this paper, instead of access control multimedia file, provides access level of data content. In fact, the use of metadata and important objects in multimedia file is investigated in secure access to the multimedia file.

In this paper first is offered the same work of security issue. Then design details of the secure model and its development, is reviewed. Finally is presented the security requirement and modeling of the proposed plan, results and offers for future work.

II. BACKGROUND AND RELATED WORK

In different aspects, there are many models that perform operation of distribution media. In this study we will focus on the following models. These models also consider the security requirements that improved the process of distributing multimedia files.

James et al [4] have presented a model based on Petri-Nets which uses multilevel security mechanism. This model, take into account multiple classify of media objects, also is considered multimedia synchronization requirements and is provided the classification level of control over user-defined multimedia documents. In fact, allows many security restrictions and the hierarchical classification policies.

Kim et al [5] have represent operating system modules based on client/server structure that is used agent module to give services and provide security. In user side to improve security and system performance, a security agent is considered to provide decoding operation and implementation media content. The security agent uses a group of symmetric keys, so if a key is exposed, without knowing the other keys, cannot be encoding all content. As a result, the risk of attack to system is reduced.

Striletchi [6] have purposed Web-Matrix developed framework that is considered all security aspect in distribute learning and commerce applications. The framework includes several modules that make it easier to perform final product. Also provides management many online users to access data in database.

Obviously, the composition methods and works can be obtained approaches and models which is more efficient but to achieve a safe and organized framework, in this study, we use

related concepts of Web-Matrix that has a high error tolerance for future changes and applications development.

III. Proposed General Plan

This paper provides a model that is provided access to authorized services based on the customer's credit. The purposed model based on development Web-Matrix framework that is can be change within requirement of specific systems or applications. The multimedia data saved in a secure repository (such as file servers) and security associated information is controlled by database manager. The database manager, using the existing modules, extracts media objects and metadata information and stores in the metadata database. Then, each object is assigned to security classify that be sent only authorized object of the requested media.

We attempt to use capability of multimedia database for management and extraction metadata from media files that improve secure data transmission in Stand-alone applications. The method in this study to data access control presented with browser. The first step is providing a secure Web server that all files are located in the main form. Also information of files, include price data, metadata and media objects are stored in the server.

When the user wants to access the existent files, first register his properties in web server and obtain a public key. The key will be used for encoding files. On important parts of the media, partial coding is done. With purchase credit and perform key, user can convert encrypt area of files to original quality. Also for copyright protection a watermark is embedded in files that used in prove the product owner and identifying unauthorized copies that is shown in Figure 1.

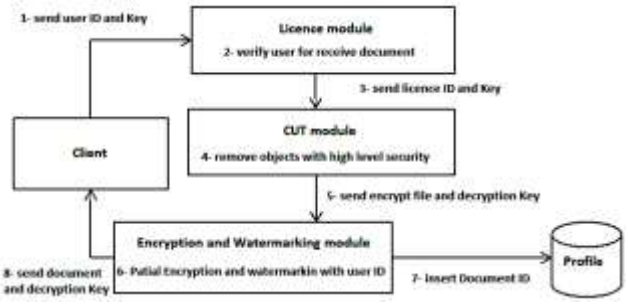

Figure 1. Steps of encryption and watermarking

This process based on the Web-Matrix structure, perform in three levels, that model provide the security requirement. Separate control modules, ensure data security.

- The first level is graphical user interface, a layer includes software components that load in the client machine and connected to the server to offer application base on Web-Matrix.
- The second level is the core application. The software modules control user interface. This layer is involved with all activities should be made to access a file. It also defines the database management module.
- The third level shows applications database. This layer is involved with activities such as object selection and classification of objects in the database. These activities are done through a secure interface that accesses the database. Details of the proposed model, is shown in Figure 2.

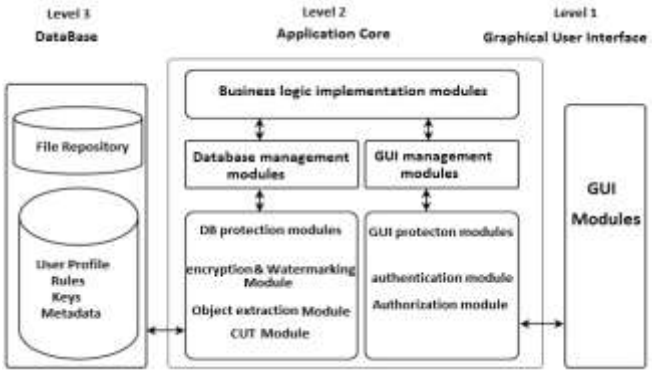

Figure 2. Exist modules in the propose plan

Security activities, as far as possible, distributed that single points of failure will have minimal impact in security system. Lines show the flow of information between model components. Security policy based on mandatory and discretionary policy or a combination of both is emphasizes on create objects time.

A. *development model*

In the developed model, user can install plug-in software on your machine. Requests are done through the plug-in to ensure user access. With a media request, the user name and a timestamp using the user public key is sent the web server. When the Web server decode message with user public key, the validity of the timestamp is examine that user is verify.

The plug-in software, multimedia shows files and related information to coding form. The patch ensures that the user performs an operation such as decoding file, has access rights. When the user wants to perform the operation decoding, the request is sent to the web server is verified user license. With user confirm, decoding key is sent to plug-in that decoding file to the main form of media, and displayed file. Send file is watermarked with the customer information, and use to prove who created the unauthorized copying.

IV. Security Evaluation And Proposal Modeling

System security evaluation, one of the most important methods to be solve system security requirement. The evaluation process is determined, whether the system achieve desirable features against threat. In addition, the security evaluation requires exact definition of security. Access control, network security and malicious software detection are considered in system security evaluation [7].

In system security evaluation, behavior of system, attacked resources and security features of the system is determined. Security requirements should be analyzed based on resources, protection services, and security threats on the equipment and

services. Figure 3 shown clear links between resources and services that is vulnerable by the security threats. So to protect vulnerable resources and services, security requirements derived and can be used from the security mechanisms to counter these threats [8].

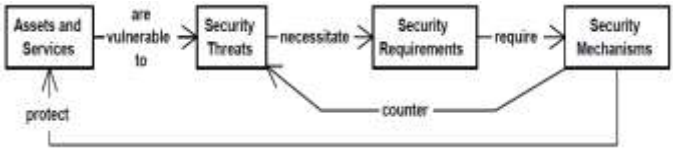

Figure 3. Relationship between security threats, system requirements and mechanisms, with resources and services [8]

Many studies have been done in terms of achieving security goals that each has suggested frameworks and mechanisms to meet certain security systems. We use modeling of security requirements, that its benefits are investigated in reference [1].Modeling provide analysis of system security requirements and enabling them. Security objectives of system security requirements should be applied to a specific system and an agent does not implement them. Five goals of main security goals exist that include [9]:

- Integrity of data means that information is allowed change only in a specific and authorized way.
- Confidentiality: The information content is protected from unauthorized disclosure (using encryption).
- Authentication: The identity of the system has been proven by credible evidence.
- Availability: refers to the system resources used by the entity is authorized.
- Access Control: Access rights with respect to the objects, provides the ability to use resources.

Modeling helps to analyze system security, support of logical evaluation and development design view. Requirements engineering approach is presented to extraction, capture and security requirements analyze.

This approach can play an important role in the discovery and security requirements. We are using KAOS method, for modeling security requirements. This modeling method makes that plan it easy to understand for the other areas. Then, safety of proposed model is evaluated and its security requirements are modeled.

A. security requirements in the proposed model

The model shows that objects of media file in the database, are assembled based on security classify by the database management module. Less important parts of the original file are not considered during this process. So only fields remain for security classification that are available with existing license. Although in proposed model logical access control is provided, however to access content stored in the repository take place security plan. The requirements are needs for establish private security activities. Each layer has its own requirements:

1) **Security requirements in GUI:** ***Should be guaranteed, communicate with the user establish only with GUI. Because the database manager has direct access to the database, the core application provides secure interaction between these two components by a secret key. This will ensure that only encrypted data from the database manager is sent to the user interface. If the user have a certificate, using this secure interface for communicate with database manager. Data transfer between client and server should be done the safest possible way. The only way to communicate with customers is through Web forms. Electronic form is software entity that allows users to send or receive certain data [10].***

2) **The core application security requirements:** ***Modules in the Application core, control user interface and database. Protection modules of user interface, must ensure that the entity requesting no direct access to the main database and will receive objects that have access right to it. Database management modules, too must ensure that all data are secure transferred to the database. Also respond to entity requests, only takes place through the user interface.To ensure confidentiality of data, communication between different components of the model must be encoded. Ability and type of used encoding, depending on the implementation which may be different on communication line to another. To prevent attacks on the server or client encryption based of symmetric keys is more efficient. Entity that creates or modifies the media objects (such as system administrator) should be verified correctly. For Copyright protection of content, user ID watermark in files, that offenders are identified from unauthorized release.***

3) **Security requirements in database layer:** ***Database manager, controls data is encrypted in store or retrieval media objects. Limited communication is established between database and repository. It is better if two components to be configured in internal network, that do not have access in public network. Server that has Database must provide respond to input requests.From a security point of view, all data in the database encrypted,***

data is decoding only in request time. Since the model developed, user interface on the client computer must be confidence, that the customer will have no access to files during the authorized process.

B. Requirements Modeling with KAOS methodology

Modeling methods make it possible that before system implementation, security requirement to be identified and estimated. The model is constructed so that specifies attackers, goals and their ability and system vulnerable points. The model against potential attackers should be built expertly to predict the security requirement for countermeasures. Requirements engineering approach is necessary for extracting, recording and analysis of security requirements. In this case, target requirements engineering can play an important role in the discovery and found security requirements. Today, there are modeling methods and languages can be used for modeling security requirements. Our study uses the KAOS method as a diagnostic technique in the application level. This method supports a wide range of requirements with a focus on security aspects, and allows security requirements to be modeled systematically and progressively [11]. The KAOS Goal-Oriented method based on the integration of four complementary views describing not only the future system and its environments, but also analyzes the existing system and its environment. Details of these views include [11]:

- *The* view *on the objectives.* The objectives can be refined into sub-objectives. The parent objective is explicitly linked to its children objectives. In this view links existing between objectives and obstacles that can occur against objectives can also be displayed.
- The *view on the application domain objects.* This view describes the objects, relationships, and events of the system and of the environment. It is compatible with UML object diagrams in many points.
- *The* view *on the agents.* This view describes software and human agents of the system and of its environment. The responsibilities and capabilities of each agent are modeled through the use of the "responsibility" link between an agent and a requirement that must be made fulfilled by this agent, and the "capability" link between an agent and operations it can perform. Each requirement must be under the responsibility of exactly one agent.
- *The view on the operations.* Objectives are eventually refined into operational software requirements. The formalism used to describe the operations is similar to a pre/post-conditions based formalism. In this view the specific requirements are explicitly linked together through an "operationalization" link.

KAOS methodology implemented with success in Objevtiver comprehensive tool, which provide a complete description of measures provides by the analyst.

1) **The main steps to Elaborate**

To achieve higher security, security requirement must be fully exploited. With recognizing the high level goals, can be extracted requirements and assumptions. In terms of abstraction, goals are placed in two categories [12]:

High-level goals are more general properties and thus need more agents to satisfy.

- Low-level goals are technical properties and need fewer agents to satisfy are needed.
- Higher level goals in the graph refined by the agents are achievable by operations.

If sub-goal set together satisfy a goal; is used abstraction "AND" and if use alternative sub-goals, is used "OR" refined. When any of sub-goals, achievable by only an agent, finished goal refining. The result of this process, different end goals exchange to requirements or depending on assumptions, made in assignment. The main steps that need to extract information from high-level goals to be followed by KAOS, as follows:

a) **Build the goal model and identifying and removing obstacles:** ***In the first stage of the detailed design process is modeled system security concerns. We will survey general requirement of security with detailed. This means that security in other domains can be generalized and are implemented. The process of identifying goals and communicate of their, through refinement links is generally a combination of top-down and bottom-up sub-processes. The children goals are identified by asking questions about "how"; however the goals of parents asking questions "why" are considered the goals and operational requirement.***

With investigate security goals, refinement and analysis conflict and security obstacle. Identifying threats are identified and resolved security leakages that are causing these threats. In our model, since the goal is create a security system, the first goal security will be build security at system in high level. The security of the general aspects of security such as authentication, confidentiality, access control, data integrity and system availability, will be reviewed. Therefore all of these goals should be refined. In Figure 4, refinement of the main goal "high-level security system" is shown.

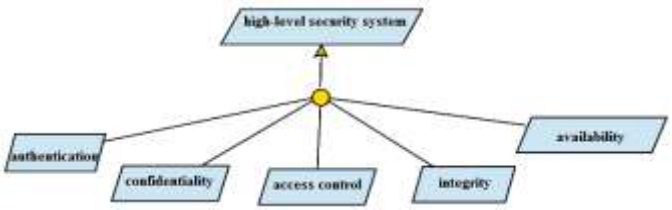

Figure 4. Refinement of high-level security system

Because these goals cannot be achieved at once, must be decomposing to sub-goals. In this stage with KAOS method that is based on requirements engineering goals, the goals refine and then extract requirements.

- *Refinement of authentication goal:* in study model, the user authentication means that user in system correctly identified and authorized. Therefore required user checking, that actual user is detected. The user authentication is possible via login ID and password and using identity proven device.
- *Refinement of confidentiality:* the reliability or privacy, a feature that shows important information about the system, such as content, services and transmitting messages, is not available. Also non-authorized persons do not have access private entities or process. In the study, confidentiality refined in two sub-goals, confidentiality of information systems and confidentiality of messages and user requests. The confidentiality, not only is required use of information encryption, but also is needed security controls at the client side and server. Any message is transmitted in the system is coded that messages cannot be read to the attacker in network.
- *Refinement of access control:* access control is included ensure of authentication and provide the license. In this study, access control means that the user account is accessible only by the user. User requests are examined based on user licenses. If approved the permit, private keys of access is sent to the user. Also the purpose of copyright protection, user ID in the file is marked hidden. If the user does not have permission required to access files, important objects of files will be encrypted.
- *Refinement of data integrity:* integrity, the feature that shows the contents of database services or resources, not be altered or destroyed by unauthorized users. Transferring messages may have not changed in transfer, either accidental or unintentional. Also integrity must be providing proof, necessary to identify the sender. In our study, we will be considered data integrity on storage and messages transmitted between the client and the system.
- *Refinement of availability:* allows a Web service applications detect attack in services and do possible repair to continue service operations. In the systems study, availability means that the system is known by all users and resources whenever receive with authorized users. In addition to identifying the attacker, use of log files in transactions, improves accountability of system.

b) **Assignment of responsibility requirements to Agents:** ***Responsibility model is built using the goal model. This model is characterized by each agent, which is responsible for fulfilling the requirements. The final goals are transferable to a single Agent. Agents assigned to the operation, it is committed to ensuring the ultimate goals. The requirements, as a final goal, should be assigned to a software agent. Figure 5, for example, shows responsibility model to satisfy requirements of the user interface.***

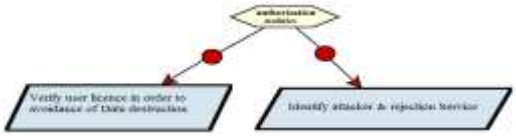

Figure 5. Responsibility model of user interface Agent

c) **Extract the object model:** ***Identify the objects involved in the goal plan, define their conceptual links and describe profile, in this model takes place. Considering each of goals is build object model. For each characteristic of an object, necessary conditions are presented to relevant Agents. These conditions depend to the application environment. Figure 6, displays the objects in the system, communication between them and system Agents.***

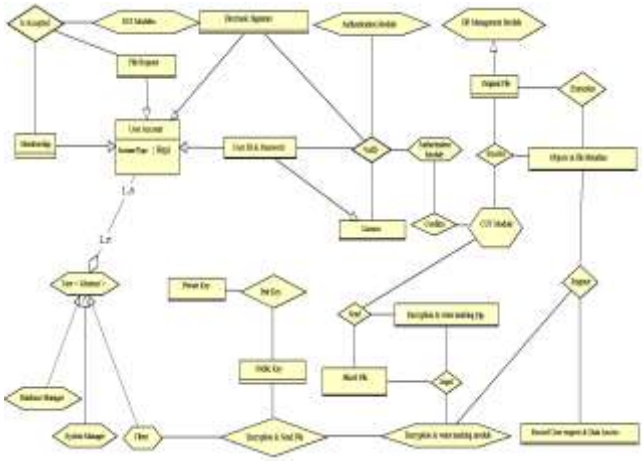

Figure 6. Modeling objects involved in achieving security goals and relationships between those

d) **Operation model:** ***Operation model is relevant to identify the object transfer state. The goal plan shows a desired or forbidden state, which is available in state transition. To determine state transfers, identified previous and next required operation and determined Agents that can perform these operations.***

For instance, when occur client connection event, activated enter requested details operation, that will receive user ID and password entities. This entity in next operation, that is register request, registered user's access. Then operations, is examined to be determined Agents that must be fulfilled operations. For example, the enter details request operation and register access request, takes place by user interface. In Figure 7, specified the Agents to perform the operation in system.

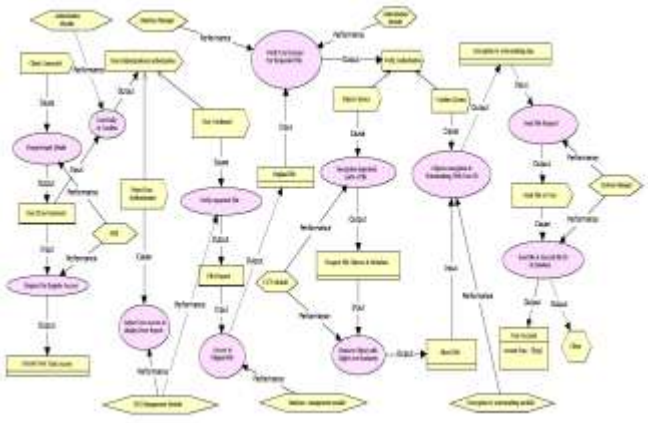

Figure 7. The responsibility of operation in system

e) **Operationalization of the requirements in the operational model:** ***Finally, in order to complete the KAOS model, must be operationalize (i.e. fulfill) requirements. Also requirements in the final level of graph must be determined by which operations are estimating. So to ensure that fulfill all goals of the system, requirements are assigned to this operations. At this level, all requirements are known and operation is identified that is responsible for implementation. We must determine how each operation to assign its requirements. With specific response, the agents operationalize requirements. Each agent for operationalize requirements that has responsibility, do operation or operations.***

So in order to analyze security of proposal plan, refinement security goals as authentication, Confidentiality, integrity, availability and Access Control, were examined threats. This modeling may provide different modes of decision making, and ensure secure plan and fulfill security requirements.

V. CONCLUSION

In this study, we propose a security model that can be used to design a framework for distributed multimedia system. The main challenge is secure access to high-resolution content and accessibility in of distributed environment. We focus on security and privacy in multimedia systems.

Protect the multimedia content in distributed environments, based on partial or progressive encryption and watermarking. For access control in distributed environments used of models provides access based on user authentication and content security features. Efficient model is multi-level security that allows users to assign different levels of data.

Models which have provided security elements in distributed environments most of all are GCOPN model, and Web-Matrix development framework. This article based on Web-Matrix development framework that is provided possible extraction and access to multimedia objects. Implementation of framework is parameterized that reflect versatility and adaptability attributes. Due to its flexible structure, new challenges resolved successfully and used to improve the facilities in future.

The structure of the original model can be used to ensure access control for all kinds of multimedia files in content-level. Difference is in the details components of model.

Security evaluation requires exact definition of security. Without specify system security requirements and attacked point, cannot properly responded to this question whether the system is secure? Therefore it is essential to be identified system security requirements.

We have modeled security requirements of our plan Aspects of user verification, confidentiality, access control, integrity and availability. In this study, KAOS method has been used as a diagnostic technique at the application level.

This method is based on goal-oriented requirements engineering that during the engineering activities, fulfill required aspects of security. KAOS method starts of understanding the system goals and ends with formal definitions of the important parts of system. The main advantage of this method is providing a continuous connection between the security problems and expected solutions. This feature is implemented in order to manage the requirements and obstacles.

The model requirements evaluation, guarantied identification and removal system threats and the model will lead to building. Also design goals of the model are developed correctly. With regard to commercial applications, in addition to providing multi-level access control, guarantees privacy of information. Implementation model, improving extraction object modules, partial coding and watermarking can be considered as further research.

References

[1] E.T. Baadshaug, G. Erdogan, and P.H. Meland, "Security modeling and tool support advantages," 10 International Availability, Reliability, and Security (ARES), ISBN: 978-1-4244-5879-0, pp. 537 - 542, 2010.

[2] ISO/IEC FDIS 27000, "Information technology – security techniques– information security management systems overview and vocabulary," ISO copyright office. Geneva, Switzerland, 2009.

[3] H. Todoran, "The road to real multimedia databases emerging multimedia data types," Studia Univ, Informatica, Volume XLVII, Number2, 2002.

[4] B. James, D. Joshi, L. Kevin, H. Fahmi, B. Shafiq, and A. Ghafoor, "A model for secure multimedia document database system in a distributed environment," IEEE transactions on multimedia, Vol. 4, No: 2, 2002.

[5] J. J. Kim, K. H. Lee, S.Y. Min, and J. G. Jee, "Multimedia contents security by wireless authentication," Lecture Notes in Computer Science, Emerging Directions in Embedded and Ubiquitous Computing, Vol. 4097, PP. 936-945, 2006.

[6] C. Striletchi, "WEB_MATRIX - A secured framework for developing businessto-client web applications," 11th IEEE International Conference on Intelligent Engineering Systems INES, ISBN: 1-4244-1147-5, pp. 1-4, 2007.

[7] J. Bau, and J.C. Mitchell, "Security Modeling and analysis," Security & Privacy, IEEE, ISSN: 1540-7993, Vol. 9, NO:3, pp. 18 - 25, 2011.

[8] D. Firesmith, "Security use cases," Journal of Object Technology, vol. 2, no: 3, pp. 53-64, 2003.

[9] I. Kotenko, M. Stepashkin, and E. Doynikova, "Security analysis of information systems taking into account social engineering attacks" 19th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), ISSN: 1066-6192, pp. 611 - 618, 2011.

[10] C. Striletchi, and M.F. Vaida, "A distributed solution for restraining the web-bots access to on-line software applications," 4th International Symposium on ISCIII, ISBN: 978-1-4244-5380-1, pp. 69 – 73, 2009.

[11] E. Delor, R. Darimont, and A. Rifaut, "Software quality starts with the modelling," CSSEA03-DELOR-CEDITI1, 2003.

[12] L. Desmet, B. Jacobs, F. Piessens, and W. Joosen, "Threat modeling for web services based web applications," conference on communications and multimedia security (CMS), pp. 131-144, 2004.