DESIGN AND IMPLEMENTATION OF A POLICY-BASED SERVICE-ORIENTED DRM SYSTEM

Yung-Hsin Wang, Dept. of Information Management, Tatung University, No. 40, Sec. 3, Zhongshan N. Rd., Taipei City 104, Taiwan, ROC, +886-2-77364785, ywang@ttu.edu.tw
Yu-Hong Lin, Dept. of Information Management, Tatung University, No. 40, Sec. 3, Zhongshan N. Rd., Taipei City 104, Taiwan, ROC, +886-932754262, yhlin00001@gmail.com
Shing-Han Li, Dept. of Accounting Information, National Taipei University of Business, No. 321, Ji-Nan Road, Section 1, Taipei City 100, Taiwan, +886-2-22326571, shli@ntub.edu.tw

ABSTRACT

This study remodels the DRM system using Service-Oriented Architecture (SOA) methodology to promote interoperability between service modules in the DRM system. It is challenging to realize SOA with web service technology while taking account of privacy and authorization requirements and capabilities. In this study, processes of all security needs in the service-oriented DRM system are policy-based and are built upon eXtensible Access Control Markup Language (XACML) standard to enable standard, generic, distributed and flexible security architecture. The resulted Web services such as those of digital contents authorization, enquiry, and information access are developed so as to increase the efficiency of content management and policy reusability.

INTRODUCTION

In recent years mature digital technology and Internet has allowed digital contents to be accessed via any popular easy-obtained devices ranged from personal smart phones and tablets to commercial digital signage and kiosks. On the other hand, digital contents are vulnerable to be speedily copied and disseminated. In order for the copyright of digital contents to be respected and controlled, applying DRM (Digital Rights Management) technology to legitimately use and proper manage digital contents seems to be of vital importance for content providers.

Business operations in general DRM application get involved with (1) Content Providers (Publishers) who provide digital contents, (2) Distributers (Portal System Operators) who are in charge of sales and marketing, and (3) Trusted Third Parties (Clearing House) who ensure adequate protection, auditing and clearing for digital contents and copyright [8]. This study aims to deliberate on re-modeling DRM system based on SOA (Service-Oriented Architecture) for all participants to be well collaborated and equitably share sales benefits of digital contents.

SOA is not only a framework but also is regarded as a key mechanism producing cost effectiveness. It promotes organizational agility to adapt the most frequent changing environment [2]. Implementing SOA technology to improve DRM systems can achieve service interoperability and loose coupling compliant with open standards, and to reuse or compose shared service components during service orchestration. Hopefully all parties within the system of DRM application are able to integrate their own legacy systems to obtain new business SOA solutions.

In DRM system, besides access control of digital contents, there are a lot of variable resources provided by all participants: content providers support digital contents, related information and copyright, portal
system operators own information of their users and distribution channel, and trusted third parties ensure legal use of digital contents and account clearing. The issues of secure access in many application systems are well known. Therefore, how to design the security policy in a unified manner and abstract it from the system to enable standard, generic, distributed and flexible security management is another focus in this study.

Most DRM systems implement access control and authorization in their own proprietary manner, which results in extreme tight coupling of authorization decisions within applications. With embedded authorization, it becomes virtually impossible to reuse security components by decoupling contract and even obtain a consolidated view of the policies protecting various resources of DRM system. This study introduces the eXtensible Access Control Markup Language (XACML) [7] technology to decouple authorization decisions from DRM system. We shall illustrate how XACML is used to define each party’s security policy of the DRM system so that the flexible policy-based SOA solution would be able to fulfill autonomous management on mutual authorization and access control for all resources.

BACKGROUND AND TECHNOLOGY

DRM system and SOA concept

DRM system emphasizes on protection and management for digital contents. However, as shown in Figure 1, the essential purpose of DRM system is to control publication, billing/payment and copyright for digital contents [6]. The participants include:

- Content Providers, who are owners of copyright of digital contents and the demanders of copyright protection.
- Distributors, who are licensees to sell digital contents on the property of copyright owners. They also provide their store channels to distribute digital contents. Those channels can be either online stores or any kind of shopping websites.
- Consumer, the users of digital contents who use Distributors’ store channels to consume and fetch by downloading or streaming legal digital contents.
- Clearing House represents trusted third parties who are responsible for handling the transaction records clearly and sharing profits fairly.

Cryptography-based and watermarking-based protection schemes are two commonly used technologies for DRM; however, interoperability problems arise within different solutions [4] [5]. Figueira Filho et al. [4] in their proposed framework adopted SOA and a high-level policy modeling approach to promote interoperability among DRM systems; however, the policy model only focused on the copyright protection. The DRM system is often combined with certain business models for the sales of digital contents. Figure 2 shows the integrated solution of DRM technology where digital content business operations are fulfilled in each server. As shown in Figure 2, the DRM platform is highly complex and extensive where a diversity of devices, media, functional modules, and a wide variety of system requirements regarding security, flexibility and manageability must be supported.

SOA as a design concept is similar to the legacy system analysis and design and system development life cycle (SLDC). However, it is based on business process in mind with a set of service oriented design principles: Service Contract, Service Loose Coupling, Service Abstraction, Service Reusability, Service Autonomy, Service Statelessness, Service Discoverability, and Service Composability [2] [3]. With its features SOA is undoubtedly able to bestow better solution on DRM systems.
XACML frameworks for web services security

Typically Digital Right Expression Language such as ODRL (Open Digital Rights Language) (ref. to http://www.w3.org/community/odrl/) or XrML (eXtensible rights Markup Language) [9] is common solution for the access control of digital contents. When the DRM system has adopted SOA, the platform shall support functional requirements with web services. Accordingly system security, privacy, resource authorizing and access control must be well managed. To deliberate such subjects, this study uses XACML to express security policy for resource authorization and access control among systems. Security policy helps participants autonomously manage their own systems. This study also emphasizes the abstraction of security jobs from the logic loop of business system to become public services to achieve centralization of operation and management.

To ensure confidentiality of authorized access and information security of service resources on SOA, OASIS (Organization for the Advancement of Structured Information Standards) has regulated XACML as security standards to support security technology for access control. XACML is based on XML standards to define the general policy syntax for resources protection and access decision. It also integrates the attribute-based authorization mechanism to support accurate access control to resource management and Web service. Apart from XACML ensure security in a loosely-coupled SOA environment, we can count on XACML to easily interoperate with other applications using the same standard language and we can reuse XACML-based policies in many different kinds of applications.

In the implementation process of XACML and access control architecture, access applicants have to enter the checking point of Policy Enforcement Point (PEP). Then PEP makes a decision request to the Policy Decision Point (PDP) to obtain the access decision. PDP then needs Policy Administration Point (PAP), which manages access authorization policies, to obtain policy. PDP can also call on Policy Information Point (PIP) to retrieve attribution (property) values of autonomy, resource or environment. After PEP obtaining the access decision from PDP, PEP does its duty to respond requester whether the access is allowed, denied, or not applicable.

DESIGN AND IMPLEMENTATION OF THE DRM SYSTEM

This section illustrates how to establish a new SOA layer abstraction for the existing DRM system and how to apply XACML for the design and implementation of the policy-based SOA DRM system.

Step 1: streamline DRM system architecture to be service choreography
DRM system architectures vary from different needs and technologies, but the basic structures are similar. The fundamental system architecture is based on the Intertrust framework [8] which most DRM solution providers (vendors) have followed. Toward practical business application, three roles are enacted in the DRM system: (1) Digital Content Provider (CP) who provide Digital Contents, (2) Digital Content Portal Operators (PO) who are in charge of sales and marketing, and (3) Third Party Authority who ensure adequate protection, auditing and clearing for digital contents and copyright.

**Step 2: achieve the service-oriented DRM system**

This study applies Arsanjani’s Service-Oriented Modeling and Architecture (SOMA) method [1] for service-oriented analysis and design of the DRM system. The entire DRM system itself involves different functions at separated segments which are classified into different operational systems. For instance, the Digital Content Security Processing System is responsible for digital content encryption and package as DCF (DRM Content Format); the Digital Content Management System maintains related information and storage for the encrypted and packaged digital contents; the Digital Content Delivery System is in charge of secure delivery for digital contents; the CA/RA (Certificate Authority/Registry Authority) system provides safety identification to check whether digital contents are used in the right carriers (media) with proper certified license. So system functions can be divided into several modules with each module operated independently.

After clarifying relationships between each DRM function and system, candidate services of the DRM system have to be identified. We then decide which candidate services will be developed and prepare detailed service specifications for later implementation. It is important to establish an SOA layer architecture by allocating service components to proper layers. The system layer architecture as shown in Figure 3 can be viewed as two levels. Roles at upper level play as service consumers and are allocated according to participants, activities, processes and services separately. Roles at lower level play as service providers, including service components, tooling components and resources. Once everything is ready, a loose-coupled, agile, highly efficient service-oriented DRM system can be realized.

**Step 3: implement security policy with XACML**

For the DRM system which has been enhanced with service-oriented modeling and web service technologies, the privacy, authorization and access control of resources among services must be assured. Considering how to adequately address these issues, XACML policy-based security management model is used. Our policy-based SOA implementation for DRM System as shown in Figure 4 consists of three main components: Content Provider, Consumer and Distributor, and XACML Entitlement Engine. Once Content Provider makes a deal with Distributor on the contract of the content sale, the CMS will invoke the XACML Policy Converter WS to convert the specific content (Resource), the authorized Distributor (Subject) and access right (Action) into XACML Policy (as Figure 5 shows); the XACML Policy is then imported into XACML Entitlement Engine. Any maintenances of XACML Policy can be processed through the CMS of Content Provider or PAP interface of XACML Entitlement Engine. Because all the authorized contents have been registered in XACML Policies, Consumer or Distributor can use PEP to construct the XACML compatible request asking for the permission to retrieve the specific contents (Figure 6 shows the inquiry: Has op01 been authorized to sell cp01_b01 by cp01?). When gets the permission from PDP, Distributor can then present the authorized contents to the portal and Consumer can be assured for the legal use (as Figure 7 shows, Permit means op01 has right to sell cp01_b01). Note that, in this study, we use WSO2 Identity Server for the XACML Entitlemen Engine, and use Apache Tomcat as the development and runtime environment for XACML Policy Converter WS and PEP.
Figure 3: The DRM system with layered SOA

Figure 4: The policy-based implementation

Figure 5: An example of XACML Policy converted from CMS.

Figure 6: An inquiry example of XACML Request for Consumer or Distributor.
CONCLUSIONS

By means of service-oriented modeling and construction, we established the SOA layered architecture of DRM system. Relationships of three group parties among the DRM system, content providers, distributors and trusted third parties, have been changed from tight coupling to loose coupling. This makes the operation among systems flexible and react agilely, whatever in data transmission, exchange or integration. On the other hand, this study uses rules of XACML security policy to define web services (components) such as digital content licensing, queries, information access. Therefore secure access and authority control can be effectively fulfilled. The approach not only promises security control of web services, but magnificently empowers XACML policy on information inquiry for each digital content whether it is permitted to publish for sale or not. It is actually able to incarnate the loose-coupling for resources sharing. Besides, the XACML policies’ attributes can be easily reused. In general, using XACML editor to come out the policy is not easy; the method (via XACML Policy Converter WS) introduced in this study can easily derive the policy with normal information maintenance.

REFERENCES


Figure 7: The example of XACML Response from PDP regarding Distributor’s inquiry.