Abstract

Technologies for Web services provide a new architecture for applications integration inside and outside the enterprise. With the flexibility provided by the Web services architecture, truly interoperable systems can be constructed. These features are favourable for the realization of business processes for Web application. In this paper, we study the feasibility and practicability of digital rights management (DRM) implementation with Web services, and further propose a watermark-based DRM implementation with Web services that can manage watermarks and deal with involved parties in a business transaction. The benefits of the proposed implementation include better coordination and interoperability among parties, a higher information privacy and security, and streamlining processes in business. These advantages overcome some major shortcomings in existing DRM implementation in e-commerce.

Keywords: Digital rights management, Web services

INTRODUCTION

Digital rights management (DRM) prevents unauthorized use of digital files (in any format – sound, images, text, documents or data) and/or identifies the source of such use (Wayner 2000). The term ‘rights management’ refers to the process of honouring copyright provisions, licence terms and usage agreements established by the owner of the intellectual property (Anderson and Lotspiech 1995). It is important to establish a DRM system that controls the usage and distribution of distributed content, and turns all distributed content to be rights-protected content. A DRM system should protect the interests of all parties, including buyers, authors, composers and distributors.

Cryptographic-based and watermark-based protection schemes are two commonly used technologies for DRM. In cryptographic-based rights protection, digital contents are always distributed in their encrypted forms. However, when a piece of encrypted digital content is decrypted, it becomes ordinary digital content that is no longer protected and carries no rights information. To address this problem, many DRM solutions achieve rights protection by attaching a code or a tag in a form of a digital watermark that uniquely identifies both the creator and the buyer of the digital content. This indicates...
that the watermarking-based DRM solution is better than the cryptographic-based solution in this sense. This paper focuses on watermark-based DRM systems.

In view of this, Zhao (1997) proposed the use of a hierarchical watermarking scheme to cover all parties involved in electronic trading, including merchants, buyers, logistic partners and so on in the rights management scheme. Hierarchical watermarks provide evidence of illicit copying and dissemination (Utku Celik et al. 2002). Katzenbeisser (2001) reviewed the requirements of practical copyright protection schemes and surveyed protocols that use symmetric and public-key watermarking algorithms. To achieve this, each piece of content is embedded with three watermarks, namely, the public, owner and recipient watermarks. The public watermark containing traditional copyright information is encrypted with a public key, so that buyers will know the publisher of the digital content by successfully decrypting the public watermark. The owner and recipient watermarks provide information about the owner and buyer, respectively.

Many existing DRM systems employ digital watermarking as the core enabling technology for rights management (Hartung and Ramme 2000). These systems include Anderson and Lotspiech (1995), Hartung and Ramme (2000), Yi et al. (1999) and so on. Collecting the information for producing required watermarks in these systems usually involves several sequential stages, namely an offline registration process, a payment process, and a rights approval procedure. In verifying the rights, existing systems require an independent process that could rely on the client and/or the server or both to verify the rights. These processes and stages vary from application to application and from business model to business model. This limits their applicability and reduces system efficiency and user satisfaction, in particular for the online media distribution business.

The following are some of the key problems and issues that exist in DRM for Web applications:

- **Privacy and Trust:** Personal information including personal identities, keys and so on are held by different parties and are required to be exchanged when needed. Privacy becomes a great concern; in particular trust does not exist in these involved parties (Cheung et al. 2002).
- **Coordination and interoperability:** E-commerce protocols and Web technologies are usually different from sites to sites – from creators to distributors. Integrating DRM into a business with these parties needs to resolve the coordination and interoperability problem.
- **Security:** Watermark insertion and verification processes are the keys in watermark-based DRM. Protection of these processes is required. These processes should be treated as black-box processes and the sensitive information should be kept by a trusted third party, e.g., a watermark clearance house (Kwok forthcoming; Memon and Wong 2001).

This objective of this paper is to respond to the above problems and issues with a DRM implementation with Web services. The focus will be on the feasibility and practicability of the proposed implementation. The paper also discusses the benefits of the implementation with Web services.

Mohan (2002) defines Web services are self-contained, self-describing, modular applications that can be published, located and invoked across the Web, and Web services perform functions that can be anything from simple requests to complicated business processes. Web services technologies that are based on the exchange of standardized SOAP messages provide a new architecture for applications integration. Web Services are language- and environment-neutral programming models, which yield flexible and loosely coupled business systems (Vinoski 2002). Services involving buyers, service providers and intermediates can be established easily without the burden of interoperability and compatibility. With the flexibility provided by the Web services architecture, it is possible to build truly interoperable systems, and the costs for setting up business over the Internet can be relatively low.

The concept of Web services is the beginning of a new service-oriented architecture (SOA) in building better software applications (Burbeck 2000). Services must be based on shared organizing principles that constitute a service-oriented architecture (SOA), the architectural concept behind Web services. The term ‘service-oriented’ for architectures, focuses on how services are described and organized to support their dynamic, automated discovery and use. Service provider, service requester and service registry are the three roles in SOA. These roles are related by means of the key requirements of ‘service description’, ‘service publication’ and ‘service binding and invocation’. To facilitate information exchange between roles, these requirements support publish, find, and bind. Readers may refer to (Burbeck 2000) for details of service roles and interactions. Our DRM implementation with Web services is based on SOA.

DRM is important in online media distribution business. International standards for protecting rights of distributed media including Secure Digital Music Initiative (SDMI) (Kwok et al. 2000) and MPEG-4 (MPEG-4) are still under development. The findings reported in this paper may have impacts to the development of these standards. This also motivates us illustrating the implementation of DRM with Web services.

The remainder of this paper is organized as follows: the next section discusses how to implement DRM with Web services. The rights insertion phase and the
In this section, we introduce and present the benefits of implementing DRM with Web services. The final section provides a conclusion to the paper.

**IMPLEMENTING DRM WITH WEB SERVICES**

To implement digital rights management for online media distribution business, we map our client/server-based rights management system (Anderson and Lotspeich 1995; Kwok *et al.* 2000; Liang *et al.* 2002), which resides in the clearance house into the Web services framework. In such an implementation, two technical issues are to be resolved and they are: (i) the role of a DRM system in an e-commerce transaction within a Web services environment; and (ii) how a DRM system using digital watermarking technology can be integrated into a Web service environment. We propose two corresponding phases to ensure DRM: the rights insertion phase and the rights verification phase. In the rights insertion phase, rights information is embedded in digital content as watermarks. The resulting watermarked digital content is then distributed to the buyer. In the rights verification phase, a designated DRM technology provider inspects the embedded watermarks. *Rights insertion operation and rights verification operation* are handled in the Web service architecture.

**Roles of the Watermark-based DRM System**

Trust is a critical issue in facilitating e-commerce transactions over the Internet since, in most cases, trading parties do not know each other. It involves five different issues concerning various trading parties and rights management phases (Cheung *et al.* 2002) as shown in Table 1. These issues must be resolved before wide acceptance of e-commerce will take place.

However, such issues of trust are generally not supported in most e-commerce frameworks. It is therefore the role of a DRM system to establish various types of trust on the top of the framework. The trust issues concern both the rights insertion phase and rights verification phase. For a watermark-based DRM system, these two phases are driven by the mechanisms of watermark insertion and watermark verification as shown in Figure 1.

The watermark insertion mechanism is concerned with the insertion of watermarks into digital content and their reliable distribution to buyers. Suppose we have a digital content, $X$, a watermark, $W$, and a secret key, $K$. A piece of watermarked content, $X'$, can be generated.

**Table 1. Various issues of trust in e-commerce transactions**

<table>
<thead>
<tr>
<th>Rights management phase</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rights insertion</td>
<td>Buyers cannot be trusted</td>
</tr>
<tr>
<td></td>
<td>Merchants cannot be trusted</td>
</tr>
<tr>
<td></td>
<td>Content providers cannot be trusted</td>
</tr>
<tr>
<td>Rights verification</td>
<td>Buyers cannot be trusted</td>
</tr>
<tr>
<td></td>
<td>Content providers cannot be trusted</td>
</tr>
</tbody>
</table>

**Figure 1.** The mechanism for (a) watermark insertion and (b) watermark verification
\[ X' = I(X, W, K) \]

Corresponding to the watermark insertion function, \( I \), there is a watermark detection function, \( D \), which returns a confidence measure of the existence of a watermark, \( W \), in a content, \( X' \). A watermarking technique is referred to as **non-blind watermarking** when its detection function, \( D \), requires knowledge of the original content, \( X \), i.e.:

\[
\begin{align*}
D(X, X', W, K) &= \text{true} & \text{if } W \text{ exists in } X' \\
D(X, X', W, K) &= \text{false} & \text{if } W \text{ does not exist in } X'
\end{align*}
\]

There are two situations in which such a rights management system can be used in e-business. In the first situation, the content distributor of digital content inserts a unique watermark into the content. If, at a later stage, a copy of the content is found, the content distributor can prove its rights by the existence of its unique watermark in the contents. In the other situation, content distributors can insert a unique watermark to each authorized digital copy to identify its buyer. Therefore, if an unauthorized copy is found, the original buyer of that copy can be traced. A comprehensive treatment of trust in watermarking protocols can be found in (Cheung et al. 2002).

**Integration of the Rights Insertion Phase into Web Services**

The phase of rights insertion can be integrated into the Web services by implementing an XML message exchange (shown in Figure 2) based on the typical SOAP protocol section (Box et al. 2000) in the Web services.

Figure 2 shows the message exchange among involved parties in an online media distribution business in facilitating rights insertion. Before the process begins, the creator, the distributor and the buyer need to register with a trustful third party – a clearance house (Kwok forthcoming). These three parties submit their personal identities and other information (e.g., bank account information). The personal identities are mainly used for watermarking processes in this case, while the bank account information is used for payment. The information is held in the Rights Management Database (RMDB). The rights management server (RMS) also resides in the clearance house.

The buyer is also required to register with the portal in order to begin shopping. Like usual shopping procedure, it starts with catalogue browsing at the portal. When a digital media content is selected, the buyer will be forwarded to a designated distributor. The distributor starts to process the order and prepare a rights-protected media content. The clearance house is responsible for rights management processes because all parties trust it. When the rights-protected content is ready, the clearance house will pass it to the distributor for delivery.

The rights insertion process can be a Web service as shown in Figure 3. DRM technology providers publish their DRM products to the Service registry, which run a private Universal Description, Discovery and Integration (UDDI) service trusted by both DRM technology providers and the clearance house. The clearance...
house selects the most appropriate rights insertion process and provides the required information to the associated technology provider for rights insertion. The selection of the rights insertion process depends on several factors, including the capabilities of the buyer’s player, the nature of a song and the preference of the content distributor.

**Integration of the Rights Verification Phase into Web Services**

The rights verification phase involves three parties: the licence holder, the distributor and the clearance house. The licence holder is the buyer that holds a licence for using a piece of rights-protected digital content prepared by a clearance house. The corresponding clearance house is responsible for licence verification. Since the distributor is also involved in the rights insertion phase, it also plays a role in verification.

The licence verification actually takes place at the designated clearance house. The location of the clearance house depends on the rights-protected media content being examined and the record of the distributor. As watermarks are applied repeatedly to every fragment of the digital content, rights verification can be based on a fraction of the whole content.

To facilitate rights verification in the Web services environment, we introduce a new rights verification transaction as shown in Figure 4, called the Rights Verification Transaction, which consists mainly of:

- a Digital Rights Verification Request from a content distributor to a licence holder, specifying the information needed for verification;
- a Digital Rights Verification Response from a licence holder to a content distributor, supplying the requested information; and
- a Digital Rights Verification Status returned by the content distributor to the licence holder, confirming the validity of a licence.

Figure 4 illustrates the message exchange in the rights verification phase. The rights verification transaction starts when a licence holder opens a piece of rights-protected media content with a designated media player. The media player will automatically connect to the distributor from which the rights-protected content is downloaded. The distributor notifies the responsible clearance house and sends the content distribution service description and the location of the clearance house to the media player. On receiving the information from the distributor, the player then issues a rights verification request with required information to the clearance house. If the digital content requires licence validation, the clearance house returns a Digital Rights Verification request, which contains parameters specifying the type of information needed. The player then prepares a Digital Rights Verification Response containing the required information, which is often a portion of the watermarked digital content such as a couple of audio frames. Based on the submitted digital content, the clearance house verifies the associated licence based on the embedded watermarks. The verification result is then returned to the player through the digital rights verification status. This completes the rights verification transaction. Upon receiving a positive response, the player is allowed to open the digital content.

The rights verification phase can be a Web service. The same DRM technology will be selected for rights verification, although the technology providers could be different. It is because the DRM solutions: (i) locate in various physical sites for users residing in different locations; and (ii) support load-balancing for higher efficiency and satisfaction. The clearance house has the right to select the most appropriate rights verification process and contact the associated technology provider for rights verification.

The clearance house plays a very important role in both rights insertion and verification. It is because both the RMS and RMDB reside in the clearance house. Trust and security still hold in the proposed
BENEFITS OF DRM WITH WEB SERVICES

Coordination and Interoperability

All five involved parties, namely creators, distributors, buyers, clearance houses and DRM technology providers are beneficiaries of the Web services implementation of DRM. In addition, DRM technology providers are also benefited from such implementation.

The DRM Web services can be held by DRM technology providers, which manage and maintain the watermarking technology. The DRM technology providers do not need to worry about the protocol and platform compatibility problems among creators, distributors and buyers because DRM Web Services provides a common platform for all these parties to perform DRM operations.

Besides, the DRM technology providers may concentrate on the development of one ‘complete’ and less-buggy DRM solution for all distributors regardless of their platforms and even business models. This is because the distributors treat the DRM solution as a DRM black box and apply it to their business workflows directly. The management and maintenance of the DRM solution, in particular an upgrade of watermarking technology for higher robustness and performance, can be performed by DRM technology providers centrally.

Distributors may implement various business models, such as pay-per-view, pay-per-download etc easily with the support of DRM Web services because DRM Web services can be viewed as objects.

Buyers may end up with a single standard DRM-enabled media player to access rights-protected media content provided by various distributors. This is different from existing DRM solutions that usually require buyers to install proprietary players for rendering rights-protected media content.

Privacy and Security

Implementing DRM with Web services can improve information privacy and security. For the DRM related processes, buyer information is required for watermark generation and verification. In a typical Internet portal, Web content is actually composed of frames of Web...
pages directed to different websites. In the Web services approach, a portal implemented with Web services can cluster the services provided by different parties. The buyer only needs to provide the information once to the Web services provider and hence reduces the risks to buyer privacy. Also, the single source of buyer information ensures data integrity and improves information security.

Trust

DRM with Web services enables un-trustful parties to be involved in the business process; in fact this is common in today’s electronic businesses. The Web services platform resolves the trust concern among the involved parties because data privacy and security are usually higher in the Web services approach. The watermarking information including the choice of watermarking technology and key information are kept and processed by a trustful third party – the clearance house. Hence creators and distributors may pay more attention on their development and business, while buyers may enjoy their purchased media contents more without changing different players with different contents.

Streamlining Business Processes

DRM-protected content distributions typically involve complicated workflows that govern buyer information extraction, payment confirmation, rights insertion and rights verification. In the Web services approach, these processes can be executed in parallel in principle although control and data dependencies between these processes still exist. These processes can also be operated by different parties, for example, the rights insertion and rights verification can be operated by a trusted clearance house, payments can be processed by a corresponding bank. The services composition architecture of Web services can facilitate communication of these processes and provide the integrated confirmation.

CONCLUSIONS

This paper investigated some practical issues of implementing DRM with Web services. The proposed implementation responds to DRM problems in existing Web applications. These problems are: (i) privacy and trust; (ii) coordination and interoperability; and (iii); security. The roles and the processes of DRM in the proposed implementation were addressed and explained. The proposed implementation is realized by two corresponding phases, namely the rights insertion and rights verification phases. These two newly proposed phases explain: (i) the role of DRM in e-commerce transaction; and (ii) the way to integrate of DRM into business transaction with Web services. They also illustrate the ways we extract rights information from business transactions in the Web services environment and verify rights information from the rights-protected content online. The findings presented in this paper demonstrate the feasibility and practicability of implementing DRM to Web applications using Web services.

Our primarily evaluation of the proposed implementation shows that the proposed implementation can resolve the existing DRM problems. However, the proposed implementation with Web services is subject to the popularity and the extensibility of Web services.

Many may be interested in the performance issue of the proposed DRM implementation. However, this paper does not address this issue. This is because: (i) the current prototype is not designed for performance evaluation; (ii) current solutions supporting Web services technologies have not been optimized for high performance implementation; and (iii) watermarking processes could be more expensive (Kwok and Yang forthcoming) than Web services overheads. The study of the overall performance should therefore be mainly driven by that of watermarking processes. The performance study will be reported in our future works.

ACKNOWLEDGEMENT

This research is supported by Sino Software Research Institute (SSRI01/02. BM01).

References

InterTrust Technologies, online at: http://www.intertrust.com [accessed Nov. 2002].


