

معماری، امنیت و سرویسهای کتابخانه های دیجیتالی

رویا بهروزی

عضو هیئت علمی دانشگاه آزاد اسلامی شیراز

behroozi@iaushiraz.ac.ir

عزیز پور ابراهیم

دانشکده فنی مهندسی شهید باهنر شیراز

Poorebrahim_aziz@yahoo.com

ارائه شده در دهمین سمینار ICT کشور ۲ آذرماه ۱۳۸۵

چکیده

تسهیلات تکنولوژیکی باعث برطرف شدن یکی از موانع موجود بر نشر را تا حدی برداشته است. امروزه مطالعات فراوانی بطور افسار گسیخته در وب تولید و انتشار می یابد. کاربران جهت رفع نیازهای خود به محیط وب روی آورده اند و اغلب آنچه را که یافت می کنند معتبر دانسته و به آن منابع استناد می کنند. این مقاله به بررسی مفاهیم کلیدی معماری کتابخانه های دیجیتالی نظیر چارچوب فنی و حقوقی، محتویات و مطالب قابل ذخیره، اشیا کتابخانه دیجیتال، تفاوت شیء دیجیتالی و شیء عادی، امکانات مخازن، موضوعات مورد جستجوی کاربران و نیز سرویسهای کتابخانه دیجیتال پرداخته و درمورد ملاحظات امنیتی در طراحی کتابخانه های دیجیتالی بحث می کند، بدین علت که در این منظر قلمروی مجازی برای امنیت قائل نشده، نیاز این کتابخانه ها را به برنامه امنیت دیجیتالی مبرم و الزامی می کند، و همچنین سیستمهای پنهان نگاری دیجیتالی و مسائل اصلی مربوط به مدیریت مجلات الکترونیکی معرفی و بررسی می شود.

مقدمه

کتابخانه های دیجیتال پایدار هستند، و تبدیل کتابخانه های سنتی به کتابخانه های دیجیتالی امری اجتناب ناپذیر است، بنابراین توجهات لازم در جهت پیشبرد سیستم ها و مهارت های مدیریتی باید انجام پذیرد. برای غلبه بر ویروسهای رایانه ای و همچنین جلوگیری از هرگونه سوء استفاده باید تدابیری اندیشیده شود. برنامه ریزی کتابخانه های دیجیتالی باید مبتنی بر معماری باز باشد. به عبارت دیگر برنامه ریزی برای یک کتابخانه دیجیتالی در صورتی با موفقیت مواجه می شود که مشتریان را به مثابه مراجعان در نظر گرفته و به موضوعاتی همچون وفاداری به کتابخانه، حفظ مشتری و توسعه بازار مناسب توجه داشته باشد. در اینجا بحث گذار^۱ در مقابل دگرگونی^۲ پیش می آید بدین معنی که ممکن است برنامه ریزی برای کتابخانه های دیجیتالی بیشتر ناشی از لزوم ایجاد و توسعه منابع و قابلیت های جدید باشد، تا رشد تکاملی تراکنش های اجتماعی رایج در گردآوری، ذخیره و پردازش اطلاعات. این موضوع صرفا موجب جابجایی کتابخانه های متداول به حوزه دیجیتالی می شود. مشکلی که

¹ Transition
² Transformation

اینجا پیش می آید این است که با توجه به ماهیت کلی فناوری محور، در کتابخانه های دیجیتالی، دو موضوع پایداری و امنیت در درجه اول اولویت قرار می گیرند.

در گزارشهای پروژه فنی علوم کامپیوتر^۱ که به مدت دو سال با پشتیبانی مالی آژانس پژوهشهای تحقیقات پیشرفته وزارت دفاع آمریکا^۲ انجام شد، این طرح جهت معماری کتابخانه های دیجیتالی ارائه گردید. این معماری یک چارچوب برای کتابخانه های دیجیتالی است که در آن اشیاء دیجیتالی بسیار زیادی متشکل از همه انواع مواد و منابع بر روی شبکه های کامپیوتری ملی قرار گرفته و قابل دسترسی است. این اشیاء دیجیتالی در گزارش رابرت کان^۳ و رابرت ویلنسکی^۴ تعریف شده اند. معماری کتابخانه های دیجیتالی، حاصل بحثهای بیشمار و سودمندی بوده است که از نتایج این بحث ها هشت اصل کلی استخراج شده، در مقاله کان/ویلنسکی^۵ راجع به هر کدام توضیحاتی ارائه گردیده است. این اصول از مسائل کلیدی تبدیل کتابخانه های دیجیتالی به خدمات شبکه ای است که امروزه مطرح می باشد.

۱. اصول کلی معماری کتابخانه دیجیتالی

۱.۱- چارچوب فنی چنین سازه ای باید منطبق با چارچوب قانونی و اجتماعی باشد

جوامع حرفه ای نظامهای اطلاعاتی خود را با تمرکز بر روی نیازهای خودشان و تأکید بر دسترسی پذیر بودن و رایگان بودن آنها برای همکاران و عموم، ایجاد کرده اند. اما در آینده نه چندان دور کتابخانه های دیجیتالی درون یک چارچوب حقوقی - اجتماعی و اقتصادی وسیع تری قرار خواهند گرفت.

حوزه های حقوقی مرتبط با کتابخانه های دیجیتالی عبارتند از: حق تکثیر، حق اجرا، حقوق مالکیت معنوی، حق افترا، حقوق ارتباط حریم خصوصی و حقوق بین الملل.

این معماری قادر به تدوین قانونی نیست ولی یک طرح فنی را بیان می کند که با ساختار حقوقی مطابقت دارد. در این معماری به خالق اثر و دارنده مالکیت فکری احترام گذاشته شده و حق اثر او یکصد سال و بیشتر دوام دارد. در این معماری هر اثر دیجیتال با حقوق مالکیت جداگانه شناسائی می شود.

خالق اثر باید مسئول و پاسخگوی محتوای اثرش باشد و همچنین اشخاصی که درباره این محتوا تصمیم گیری می کنند باید رفتار مسوولانه داشته باشند. کتابخانه دیجیتالی تنها در صورتی پیشرفت می کند که برای محتوای آثار مسئولیت حقوقی در نظر بگیرند، به خصوص روی بخشهایی که تنها وظیفه آنها ذخیره و انتقال این اطلاعات می باشد. بنابراین در معماری کتابخانه های دیجیتال باید بین حوزه های مسئولیت و حقوقی با بخشهای دیگر مرز مشخصی قرار داد. در یک جمله می توان گفت این مورد بدین معنا است که چارچوب فنی چنین سازه ای باید منطبق با چارچوب قانونی و اجتماعی باشد.

۲.۱- شناخت واژگان خاص

جهت درک بهتر مفاهیم مربوط به کتابخانه های دیجیتالی باید با واژگان خاص آن آشنا بود. واژگان خاص مانعی برای توصیف کتابخانه های دیجیتال هستند. برخی از لغات در حوزه فنی یا حقوقی، حرفه ای و اجتماعی

¹ CSTR

² ARPA

³ Robert Kahn

⁴ Robert Wilensky

آنقدر معنای ضمنی متفاوتی دارند که مانعی برای بحث بین افراد با پیش زمینه و دانشهای مختلف می شود. حتی برخی لغات ساده در بین افراد مختلف معانی متفاوتی دارند. لغات خاص و تخصصی که باعث کج فهمی در بحث دقیق و جامع کتابخانه های دیجیتالی می شوند باید پالایش شود. بنابراین برای درک بهتر مفهوم های مربوط به کتابخانه های الکترونیکی نیاز مبرمی به پدید آوردن اصطلاح های فنی و تعبیر نامه های استاندارد ها می باشد. طبق معماری کان/ویلنسکی، هر مقوله اطلاعاتی در کتابخانه دیجیتالی، شیء دیجیتالی نامیده می شود که در یک مخزن نگهداری می شود. اطلاعاتی که در شیء دیجیتالی ذخیره می شود، محتوا نامیده شده که به دو جزء داده و اطلاعاتی درباره داده تقسیم شده که با عنوان مشخصه یا فرا داده^۱ شناخته می شود.

۳،۱- محدود نبودن ساختار و مطالب قابل ذخیره

پی ریزی چنین ساختاری باید بدون در نظر گرفتن محتویات و مطالب قابل ذخیره در کتابخانه های سنتی باشد یعنی جهت پی ریزی این ساختار و معماری باید محتویات و مطالب قابل ذخیره در کتابخانه های سنتی را از نظر دور کرد و همچنین باید مقوله ها و منابع و محتویات کتابخانه های سنتی از این معماری جدا شوند. در کتابخانه سنتی فقط کتاب ذخیره می شود ولی در کتابخانه دیجیتال هر نوع اطلاعاتی از جمله متن، تصویر، آثار موسیقی، برنامه های کامپیوتری، بانکهای اطلاعاتی، مدلها و ... می توانند به شکل دیجیتالی ارائه گردند. در این معماری ویژگی ها و خواص به کار برده شده برای همه انواع به طور واضحی مشخص می گردد. اعمالی که جهت حذف و یا اضافه کردن شیء به کار برده می شود، باید برای تمام انواع یکسان بوده و روش امنیتی خاص به کار گرفته شود.

معماری کان/ویلنسکی با این مشخصه ها اساس و بنیان توسعه کتابخانه های دیجیتالی است و برای انواع اطلاعات مناسب است. در توسعه تمامی فرمتهای خاص و قوانین^۲ مدیریت حقوقی که برای تمام انواع مناسب است را در نظر می گیریم.

جدا کردن عملکرد کلی کتابخانه های دیجیتالی از مشخصه های نوع محتوای آنها مزایای دیگری نیز دارد. ایجاد بازارهای مختلف و همچنین نحوه ذخیره، توزیع و تحویل محتوای اشیاء دیجیتالی از فعالیت هایی مثل تولید و مدیریت محتوای علمی آنها جدا می شود.

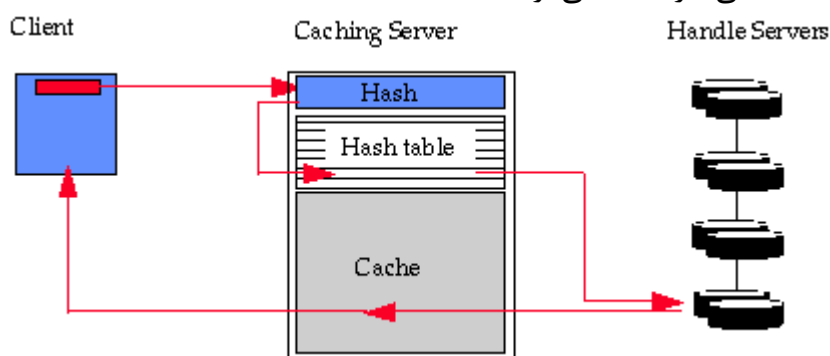
۴،۱- نام و شناسه ها اجزاء تشکیل دهنده کتابخانه های دیجیتالی

از دیگر اجزاء ساختار اصلی کتابخانه های دیجیتالی نام و شناسه است. که پایه و ستون اصلی ایجاد کتابخانه دیجیتالی می باشد. جهت شناسایی اشیاء دیجیتالی باید به آنها نامی اختصاص دهیم تا مالکیت فکری را در شیء دیجیتالی ثبت کرده و بتوانیم تغییر مالک اثر را در جایی به ثبت برسانیم. این نامها جهت بازیابی اطلاعات و استناد مورد نیاز است و برای پیوند به کار برده می شود. همچنین این نامها باید منحصر به فرد و یکتا^۳ باشند. این عمل نیازمند یک سیستم مدیریت است که در مورد شخصی که مجوز تعیین نامها و تغییر اشیاء شناخته شده را دارد، تصمیم گیری کند. این نامها باید برای یک دوره زمانی طولانی مدت معتبر باشند، اعتبار نامها باید ماندگاری^۴ داشته باشد، حتی اگر در زمان استفاده از شیء، سازمان یا شخص به وجود آورنده آن دیگر وجود خارجی نداشته باشد، برای حل مشکل نامگذاری اشیاء باید از یک نظام کامپیوتری استفاده کرد تا این مشکل به سرعت حل شود. شرکت

¹ Meda Data
² Protocol
³ Unique
⁴ persist

ملی ابتکارات پژوهشی برای این کار نظام دستگیره‌واره^۱ را اجرا کرده است. هر نشانه‌ای که برنامه جهت مشخص کردن و دستیابی به شی دیگری می‌تواند استفاده کند تا این نیازها را برآورده کند. دستگیره‌واره یک رشته یکتا است که برای شناسائی اشیاء دیجیتالی استفاده می‌شود. یک دستگیره‌واره سرویس دهنده^۲ جهانی، یک منبع قطعی برای مقاصد آرشیوی و حقوقی می‌باشد، ولی همراه با آن باید یک ذخیره پنهانی سرویس دهنده^۳ وجود داشته باشد تا کیفیت و تفکیک پذیری^۴ سریعی حاصل شود.

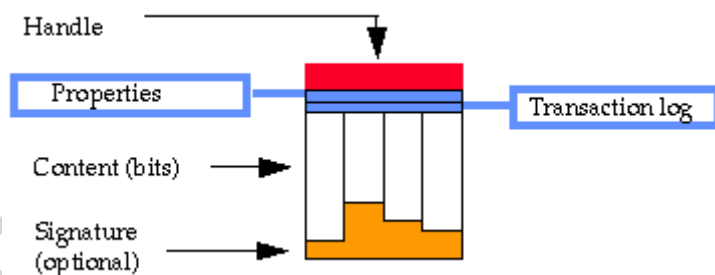
این سیستم کامپیوتری کنترل می‌کند که آیا نامهای جدید واقعی هستند یا خیر و جهت کنترل محلی نامها یک دستگیره‌واره سرویس دهنده محلی نیز اضافه می‌گردد.



شکل ۱- سیستم دستگیره‌واره شرکت ملی ابتکارات پژوهشی^۵

۵،۱- کتابخانه‌های دیجیتال وسیع تر و فراتر از محلی برای ذخیره بیت ها

در کتابخانه‌های دیجیتالی اطلاعات به صورت "شی دیجیتالی" ذخیره می‌شود. شی دیجیتالی فقط مجموعه‌ای از بیتها نیست. محتوای شی دیجیتالی دارای ساختار است که این ساختار حتی در ساده‌ترین اشیاء نیز به کار گرفته شده‌اند و اطلاعاتی از قبیل حقوق مالکیت فکری به شی دیجیتالی پیوست می‌گردد.



شکل ۲- بخشهای یک شیء دیجیتالی

برای اینکه بتوان اطلاعات سودمند محتوای شی دیجیتالی را به خوبی به نمایش در آورد، باید نوع آن بشناسیم. به این دلیل بخشی از محتوا که می‌تواند به شکل متن (شاید رمزگذاری شده به زبانهای نشانه‌گذاری از قبیل XML، HTML و ...) باشد و بخش دیگر آن می‌تواند از نوع شنیداری باشد. در یک شی دیجیتالی یکتا، می‌توانیم تعداد بسیار زیادی از انواع محتوا را بگنجانیم. به عبارت دیگر انواع داده‌های پیچیده قراردادی را می‌توان از انواع بسیار ساده‌ای ساخت که شامل توالی بیت‌ها / دستگیره‌وار و دیگر اشیاء دیجیتالی باشند و با ترکیب آنها می‌توان هر محتوای دیجیتالی دلخواه را تولید و ارائه کرد.

¹ Handle
² handle server
³ caching server
⁴ resolution
⁵ The CNRI

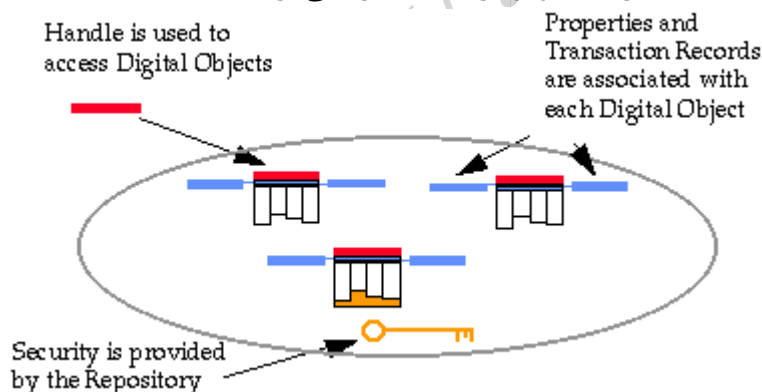
جهت سامان‌دهی مالکیت فکری داده‌ها، به فرا داده خاصی نیاز داریم که در شکل ۲ نشان داده شده است (همان دستگیره‌واره). در فرا داده همیشه یک شناسه واحد موجود می‌باشد که درون آن می‌توان مشخصه‌هایی از قبیل حقوق فکری و روشهای دسترسی را هم گنجاند. یکی از مشخصه‌ها نشان دهنده این است که آیا شی دیجیتالی قابل تغییر است یا خیر. مشخصه دیگر امضاء دیجیتالی^۱ یا روشهای دیگر تأیید اعتبار یک شی است تا آن شی را نتوان تغییر داد.

۶،۱- تفاوت شی دیجیتالی با شی ذخیره شده عادی

در کتابخانه‌های دیجیتالی آنچه که شما ذخیره می‌کنید با آنچه که دریافت می‌کنید متفاوت است. در معماری باید بین شی دیجیتالی تولید شده، شی ذخیره شده در مخزن و شی که توضیح و منتشر می‌شود به دقت تفاوتها را در نظر گرفت. محققان حقوقی به این امر معتقدند که، برای عرضه اشیاء دیجیتالی به کاربران باید بین برنامه‌های اجرایی، دیدگاه‌های کامپیوتری و اجرای مفاهیم حقوقی توازن برقرار گردد. این امر برای حقوق مدیریت کتابخانه‌های دیجیتالی چارچوب صحیحی را تبیین می‌کند، یعنی اهداف کتابخانه‌های الکترونیکی نباید وابسته به یک نوع فناوری محدود و خاص باشند.

۷،۱- داشتن امکانات قدرتمند برای نگهداری اطلاعات در مخازن مربوطه

مخازن این کتابخانه‌ها باید دارای امکانات مناسبی جهت حفظ و نگهداری ذخیره‌های خود باشد. در یک مخزن کتابخانه دیجیتالی، اشیاء به همراه محتوا و فراداده ذخیره می‌گردد.



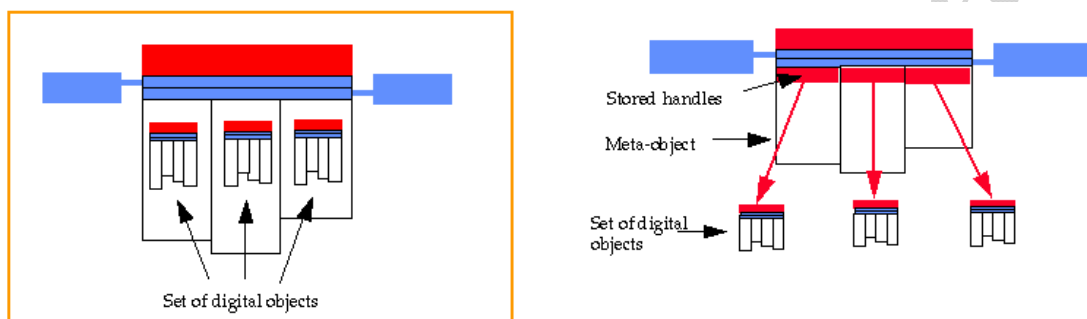
شکل ۳ - شکل یک مخزن

اشیاء دیجیتالی که در مخزن کتابخانه نگهداری می‌شود با اشیاء دیجیتالی که در کامپیوتر کاربر قابل دسترسی است، خیلی متفاوت است و همچنین مخزنهای مختلف، سازمانهای داخلی بسیار متفاوتی دارند. از آنجائی که اشیاء دیجیتالی مشمول مالکیت فکری ارزشمندی می‌باشد، بنابراین شکل ذخیره شده اشیاء دیجیتالی درون مخزن، حاوی اطلاعاتی می‌باشد که در چارچوب اجتماعی و اقتصادی مشمول قانون مالکیت فکری می‌شود. از اینرو مطمئن هستیم که فقط عملیات معتبر روی شی دیجیتالی انجام می‌شود. سازماندهی داخلی مخزن و روشهای ذخیره اشیاء دیجیتالی از دید کاربر پنهان است. برای دسترسی به مخزن کتابخانه‌های دیجیتالی پروتکلی به نام RAP فراهم گردیده است.

¹ Digital Signature

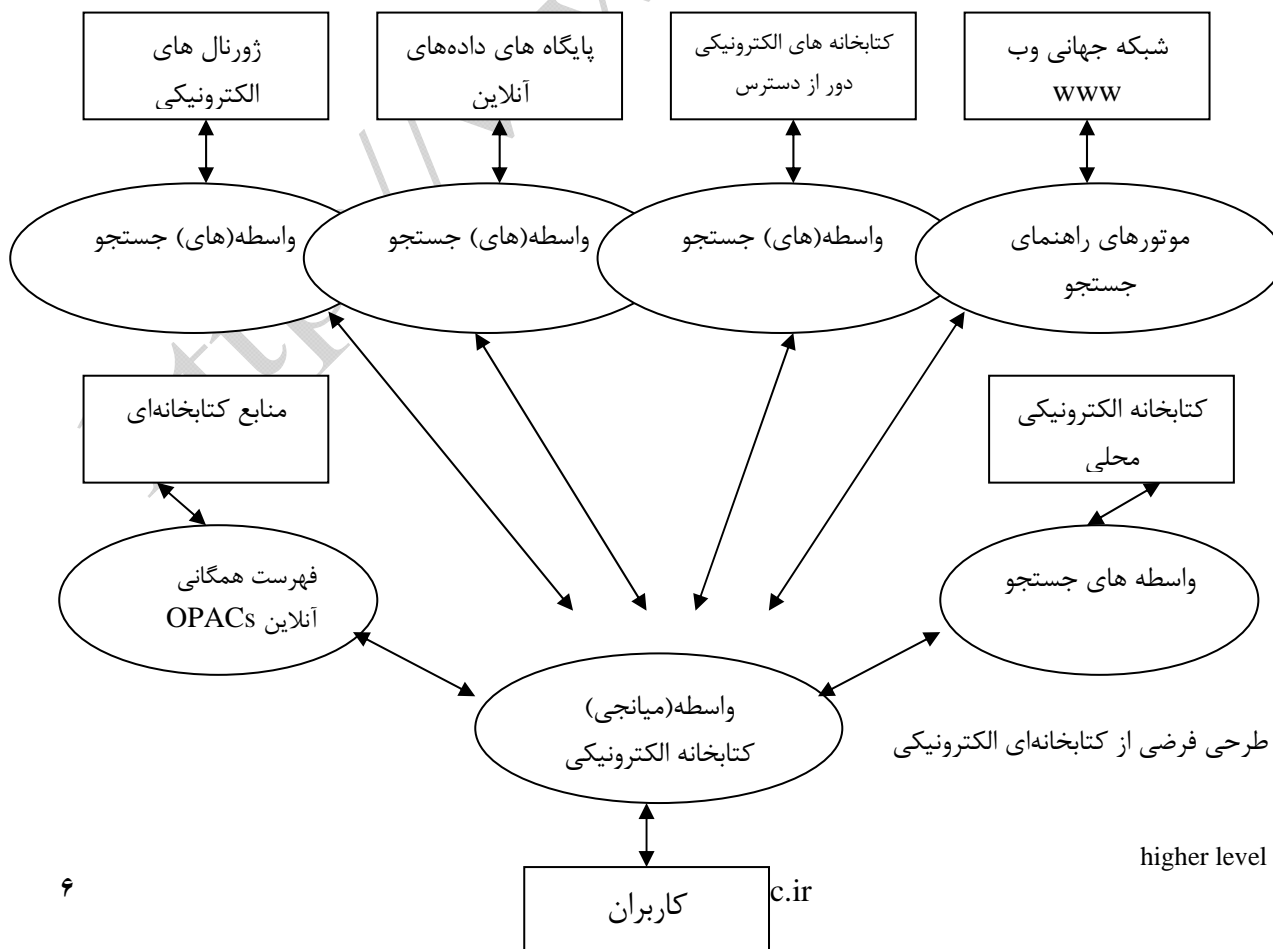
۸.۱- موضوعات مورد جستجوی کاربران

کاربران در جستجوی آثار اندیشمندانه و ارزشمند هستند نه فقط به دنبال اشیاء دیجیتالی. کاربران کتابخانه‌های دیجیتالی معمولاً به اقلامی بالاتر از سطوح انتزاعی اشاره می‌کنند. یک شیء دیجیتالی می‌تواند دارای فرمتهای مختلف، با کمی تفاوت در محتوا و سطوح دسترسی مختلف باشد، اما کاربران می‌خواهند آنها را معادل بدانند. معماری کتابخانه‌های دیجیتالی باید روشهایی را برای دسته‌بندی اشیاء این کتابخانه‌ها در نظر بگیرد و ابزارهایی برای بازیابی آنها فراهم کند. معماری کان/ویلنسی اندیشه‌های سطح بالا^۱ را به چندین روش پشتیبانی می‌کند، یکی داشتن یک شیء دیجیتالی است که حاوی چندین شیء دیجیتالی دیگر است (شکل ۴ الف) و رویکرد بعدی داشتن متغیرهایی است که به عنوان اشیاء دیجیتالی جداگانه‌ای ذخیره شده‌اند و هر کدام دستگیره‌واره خاص خود را دارند، (شکل ۴ ب) این دستگیره‌واره حاوی فرا شیء (meta object) است، که مثل یک کارت فهرست‌نویسی (catalog card) عمل می‌کند و شامل فهرستی از متغیرها به همراه دستگیره آنها است.



شکل ۴- فراشیء

طبق توضیحات فوق می‌توان یک تصویر ذهنی از کتابخانه‌های دیجیتالی را ارائه داد، که به شکل زیر ترسیم می‌شود.



شکل ۵- طرحی فرضی از کتابخانه‌های الکترونیکی

¹ higher level ideas

۲- سرویس های کتابخانه دیجیتال

۱,۲- سرویس های دیجیتال

• سرویس جستجو:

این سرویس به کاربر کمک می کند که به چهار روش, جستجو را در سیستم انجام بدهد:

الف) روش جستجوی هدایت شونده : در این روش کاربر خود انتخاب می کند که سیستم در میان چه مجموعه^۱ هایی جستجو کند. سپس سیستم نتایج جستجو را در اختیار کاربر قرار می دهد. علاوه بر مجموعه ها, کاربر می تواند پارامترهای دیگری از قبیل تعداد پاسخها و سایر پارامترها را مشخص کند.

ب) روش جستجوی بدون هدایت : در این روش این سیستم است که بر حسب شرایط , بخشی یا تمام مجموعه ها را مورد جستجو قرار داده , نتایج را در اختیار کاربر قرار می دهد.

ج) روش جستجوی مبتنی بر پروتکل Z39.50 : در این روش جستجو بر اساس پروتکل بازیابی اطلاعات Z39.50 بر روی سیستم دیگری انجام می گیرد و نتایج در اختیار کاربر قرار می گیرد. سیستم دوم که بر روی آن جستجو انجام می گیرد باید Z39.50 را پیاده سازی کرده باشد.

د) روش جستجوی Full Text : در این روش جستجو , محتویات دیجیتالی سیستم بر اساس یک کلمه کلیدی مورد جستجو قرار می گیرند و اقلام اطلاعاتی که آن کلمه کلیدی را در بر دارند ظاهر می شوند.

• سرویس بازیابی اطلاعات الکترونیکی :

این سرویس این امکان را فراهم می کند که بر اساس تصدیق اصالت مجدد (و پرداخت وجه) کاربر به محتویات دیجیتالی اطلاعات دست یابد. که این دستیابی می تواند به صورت مشاهده یا Download کردن محتویات دیجیتالی باشد.

• سرویس Browse:

در این سرویس کاربر می تواند بر روی فیلدهای مختلف متادیتای سیستم Browse کند بدین معنا که برحسب فیلد خاصی بصورت صعودی/ نزولی اطلاعات در ابتدا برای کاربر برای نمایش داده شده. سپس او قلم اطلاعاتی مربوطه را انتخاب کرده به مشاهده متن آن می پردازد .

• نتایج جستجوی ذخیره شونده:

به کمک این سرویس کاربر می تواند نتایج جستجوی خاصی را ذخیره کند و سپس در مواقع بعدی با استفاده از این نتایج جستجو, جستجو در سیستم را پی بگیرد.

• سرویس تصدیق اصالت:

بر اساس این سرویس کاربر برای ورود به سیستم و امکان استفاده از فضای تخصیص یافته به او توسط سیستم و استفاده از سایر امکانات سیستم , به سیستم Login می کند.

• ثبت نام در سیستم:

این سرویس دو بخش دارد. یکی ثبت نام در سیستم برای استفاده از امکانات مجانی سیستم و دیگری ثبت نام در سیستم برای استفاده از امکانات پولی سیستم. که بعدا کاربران در هنگام دسترسی به اشیاء دیجیتالی سیستم

¹ (Collection)

تصدیق اصالت خواهند شد. در بخش امکانات مجانی، کاربر نیازی به وجه نداشته و فقط اطلاعات خود را وارد می کند ولی در بخش امکانات پولی کاربر حق عضویت به سیستم پرداخت میکند. ضمناً اگر کاربر بخواهد از امکانات سایر سیستمها استفاده کند باید حق عضویت مشخص شده برای دسترسی به آن سیستمها را نیز بپردازد که عملاً بخش ناچیزی از آبونمان سیستم دیگر خواهد بود.

۲.۲- سرویسهای مدیریتی بخش الکترونیکی:

این سرویسها مخصوص مدیر سیستم است و عبارتند از:

- ورود اطلاعات تزاروس سیستم.
- تعریف نقش برای کتابداران سیستم: مشخص می کند که کتابداران مختلف سیستم هر یک می توانند به کدام اقلام اطلاعاتی دسترسی داشته باشند و به ورود اطلاعات بپردازند.
- ایجاد مخزن اطلاعاتی دیجیتالی : این سرویس امکان ایجاد یک مخزن اطلاعاتی دیجیتالی را فراهم می کند.
- ایجاد مجموعه: امکان ایجاد مجموعه ها را فراهم می کند.
- ایجاد تزاروس: امکان ایجاد دیکشنری تزاروس سیستم را فراهم می کند.
- تعریف کردن سیستم: بدین صورت که سیستم جدیدی که این سیستم با آن قرارداد بسته است (و از نوع همین سیستم نیز هست و آبونمان آن پرداخت شده است) به سیستم اضافه می شود تا کاربران بتوانند بر روی آن جستجو انجام دهند و در حالیکه از نوع این سیستم نیست ولی Z39.50 را پیاده سازی کرده است ، بر روی آن جستجو انجام دهند. در حالت اول هر دو نوع سیستم دو نمونه از همین package هستند ولی در حالت دوم جستجو با استفاده از پروتکل Z39.50 انجام می گیرد.
- سرویس ورود اطلاعات: امکان ورود اطلاعات دیجیتالی را به صورت مستقیم^۱ در سیستم فراهم می کند نه از طریق وب. به همراه محتویات هر قلم اطلاعات باید متادیتای مربوطه جهت قرار گرفتن در مجموعه مربوطه نیز وارد شود. و برای ورود اطلاعات کتابدار تصدیق اصالت خواهد شد و تنها در صورتی که اجازه ورود اطلاعات آن قلم اطلاعاتی را داشته باشد ، می تواند به ورود اطلاعات آن قلم اقدام کند.

۳- ملاحظات امنیتی در طراحی کتابخانههای دیجیتالی

۱.۳- امنیت در کتابخانههای دیجیتالی

اگرچه ممکن است کتابخانههای دیجیتالی را به غلط فضائی برای ذخیره سازی اطلاعات فیزیکی خاص تعریف کنند، اما رعایت ملاحظات امنیتی در کتابخانههای دیجیتالی نیز همانند کتابخانههای فیزیکی الزامی است. امنیت یک کتابخانه دیجیتالی تابعی از ساختمان مجموعه منابع، کارکنان، مراجعان آن، و صدها عامل دیگر است. این عوامل روی هم رفته موجب می شود که آن کتابخانه چیزی بیشتر از مجموع بخشهای تشکیل دهنده آن باشد. مفهومی که در اینجا به کار می رود. «امنیت سازمانی» است. امنیت سازمانی به معنای مجموعه ای از مهارتهای مرتبط به هم است، این مجموعه شامل ارزیابی تهدید، امنیت فیزیکی، امنیت عملیاتی و پرهیز از شکست می باشد. همه کتابخانهها در سوق به سوی دیجیتالی شدن، مشتاقانه با یکدیگر مسابقه گذاشته اند. بعضی از این کتابخانهها بدون اینکه به حفاظت مجموعه های خود توجه داشته باشند به سوی دیجیتالی شدن پیش می روند و بعضی دیگر به موضوعات پراکنده ای نظیر جبران تغییر نحوه استفاده کاربران، افزایش تنوع در شیوه های ارزیابی اطلاعات یا

ارائه مؤثر اطلاعات توجه دارند. رویه‌هایی که کتابخانه‌ها جهت دیجیتالی شدن پیش می‌گیرند در صورت فقدان پروتکل‌های امنیت سازمانی، بسیار ناامن و ضربه‌پذیر خواهند بود. درست است که کتابخانه‌های دیجیتالی دارای مکان واحد و خاصی نیستند، اما باز هم باید در مکان فیزیکی خاصی (نظیر دیسک سخت یا یک سرور) قرار گیرد تا بتوان آن را پردازش کرد. طرح امنیت کتابخانه دیجیتالی^۱ هم از بخش‌های فیزیکی و هم از فرایندهای تشکیل دهنده یک کتابخانه دیجیتالی تشکیل می‌گردد.

DLSP نوعی فعالیت در جهت شناخت آسیب‌پذیری‌های احتمالی، به حداقل رسانیدن آنها یا دست کم، کاهش جذابیت آنها برای نفوذگران احتمالی است. البته هیچگاه نمی‌توان به امنیت صد در صد دست پیدا کرد. آنچه که معمولاً در این راستا انجام می‌گیرد، ممیزی امنیتی جهت برجسته کردن این آسیبها است. نتایج این ممیزی باید محرمانه باشد. حسابرسی امنیتی از این دسته، در سطوح متفاوتی انجام می‌شود و کارکنان، سیستم‌های اطلاعاتی، ساختمان فیزیکی، انتشار مطالب و دستیابی به آنها را شامل می‌شود. این نوع حسابرسی دو فهرست در اختیار قرار می‌دهد:

۱. فهرست خطرات و آسیب‌پذیری‌ها.

۲. فهرست کنترل‌های ممکن و اقدامات پیشگیرانه.

این دو فهرست، ابزارهایی را در اختیار قرار می‌دهند، که به وسیله آنها برای راه‌حلهای ممکن تحلیلهایی (هزینه - فایده) انجام می‌شود.

۲,۳- محافظت از مطالب دیجیتالی

برخلاف منابع آنالوگ، همه کپی‌های منابع دیجیتال اصل هستند. فناوری جداسازی و تکثیر^۲ منابع دیجیتالی آنقدر ارزان است که در ذهن نیز نمی‌گنجد. مجوزهای گران‌قیمت نرم‌افزارها باعث بوجود آمدن رمز شکنها^۳ شده است. اکثر منابع دیجیتالی دارای محافظ‌های محکم نظیر شماره سریال، فعال‌سازهای درون خطی و ... هستند. با وجود این باز هم قفل‌شکنی می‌شوند. بهترین شیوه مقابله با این کار کدام است؟ یکی از شیوه‌ها، استفاده از پوسته امنیتی جهت ارسال مواد دیجیتالی است. پوسته امنیتی زمانی فعال می‌شود که مراجعان در همه جا به کتابخانه دیجیتالی متصل شوند و موافقت خود را در پیروی از پروتکل‌های مدیریت حقوق دیجیتال اعلام کنند. در هر حال باید توجه داشت که چنین پوسته امنیتی الزاماً با حق محرمانه بودن مسائل شخصی مغایرت دارد.

سیستم دیگری که برای ارسال مواد به کار می‌رود آریل^۴ نام گرفته است، آریل سیستمی است که توسط گروه تحقیقات کتابخانه‌ای جهت ارسال الکترونیکی اشیاء اسکن شده (چک کردن اشیاء در هنگام ارسال) طراحی شده است. در هر حال هرگاه در این سیستم، اشیاء را اسکن و ارسال کنند، دیگر به هیچ‌وجه امکان کنترل کپی‌برداری در آینده وجود ندارد. بنابراین لازم است به دنبال جستجوی شیوه‌ای برای نشانه‌گذاری مواد دیجیتالی بود که عین اینکه کیفیت آنها را پایین نیاورد، اصل بودن آنها را نیز تضمین کند. با توجه به ماهیت دیجیتالی مواد مورد نظر، چنین نشانه‌گذاری‌هایی کاملاً امکان‌پذیر است. این نشانه‌گذاری‌ها، امکان تشخیص جعل بودن مواد را در اختیار مدیران کتابخانه‌های دیجیتالی قرار می‌دهد.

¹ Digital Library Security Plan (DLSP)
² ripping
³ Code-breakers
⁴ Ariel

یکی از شیوه‌های نشانه‌گذاری، پنهان کردن داده‌های معینی می‌باشد که اصالت ماده را در خود ماده دیجیتال نشان می‌دهد، که به این شیوه پنهان‌نگاری^۱ می‌گویند.

حک کردن یک نشانه دیجیتال در یک ماده دیجیتال «فیلیگران» مهر یا نشانه‌گذاری دیجیتال^۲ نامیده می‌شود. که به دو طریق می‌توان این نشانه‌گذاری را انجام داد:

• قابل مشاهده

• غیر قابل مشاهده

در روش اول نشانه دیجیتال به طور عینی قابل مشاهده است ولی در روش دوم این نشانه پنهان شده است. مهمترین مرحله نشانه‌گذاری تولید نشانه است. نشانه شامل اطلاعات منحصر به فردی درباره مالک شیء دیجیتال می‌باشد. باید به این امر اعتقاد داشت که هرچه قدرت مقاومت یک نشانه در برابر جعل بیشتر باشد، هزینه طراحی و بازبینی آن نیز بیشتر خواهد شد. DLSP نشان می‌دهد که کدام بخش مجموعه دیجیتال نیازمند مقاومت در برابر استعمال است و کدام بخش نیاز به مقاومت ندارد. کلید این کار ایجاد توازن بین اقدامات مؤثر فعال و اقدامات مؤثر انفعالی است. برای پیگیری از تقلب، نشانه مقاومتی لازم است. با وجود این، استفاده از نشانه‌هایی که تا حدودی در مقابل جعل شدن مقاومت می‌کنند، مفید و کم هزینه است. این نوع نشانه‌ها را نشانه‌های شکننده می‌نامند. همه نشانه‌های شکننده در هنگام تکثیر بدون مجوز می‌شکنند، مگر سخت‌ترین آنها، در DSLP سیستمی وجود دارد که به وسیله آن کاربران با شناسه‌های دیجیتال که دریافت می‌کنند نه تنها قادر خواهد بود که نشانه مطالب ذخیره شده را تغییر دهند، بلکه می‌توانند داده‌ها را به گونه‌ای نشانه‌دهی کنند که تکثیرهای مجاز یا غیرمجاز را تشخیص دهند. هر مقدار که DLSP شما از پروتکل ضد جعل یا ضد تکثیر غیر مجاز برخوردار باشد، باز هم در هنگام استفاده در سیستم شما، باید دارای شرایط زیر باشد:

I. شفافیت: نشانه‌گذاری نباید به کیفیت محتوای ارسال شده (متن، تصویر، ...) لطمه‌ای وارد کند.

II. مقاومت: داده‌های نشانه‌گذاری شده باید زمانی که در معرض تحریف تا تغییر در شکل‌های متفاوت (از جمله خرابی سیستم حمل و نقل اینترنتی، فشردن سازی، رپیکسل شدن و ...) قرار می‌گیرند، مقاومت کنند و در برابر آنها مقاومت کند.

III. ظرفیت و توانایی پذیرش داده‌ها: شیوه نشانه‌گذاری باید از ظرفیت‌پذیری بالایی برای انتقال داده‌ها برخوردار باشد و همچنین بتواند - در موارد لازم - از بخشی از محیط خارج شود.

IV. کارایی: رمزگذاری / رمزگشایی داده‌های نشانه باید نسبتاً ارزان، و از نظر پردازش و محاسبه در پائین‌ترین سطح باشد.

V. امنیت: نشانه‌ها باید در برابر تغییرات و تقلبات عمدی، مقاوم باشند.

۴. مسائل مربوط به مدیریت مجموعه مجلات الکترونیکی

۱،۴- انتخاب مجلات الکترونیکی

انتخاب یکی از اصلی‌ترین عملکردهای مجموعه‌سازی است. انتخاب در متن‌های مختلف می‌تواند معانی متفاوتی به خود بگیرد. برای یک مجله، هزینه - مدار انتخاب به معنی اتخاذ تصمیم نسبت به پرداخت حق اشتراک

¹ steganography
² Digital water-marking

یا پرداخت هزینه جهت اخذ مجوز دسترسی به آن مجله می‌باشد. انتخاب می‌تواند در معنای تصمیم‌گیری جهت ایجاد دسترسی به یک مجله الکترونیکی در یک کتابخانه الکترونیکی از طریق شبکه (محلّی یا اینترنت) بکار رود. دو رویکرد نظری جهت انتخاب وجود دارد. یکی بر فرمت مجلات و دیگری بر موضوع مجلات استوار است. در رویکرد فرمت - مدار، انتخاب مجلات الکترونیکی توسط کارمندان که از مهارت‌های کافی در زمینه منابع الکترونیکی برخوردار هستند انجام می‌شود. ولی در رویکرد موضوع - مدار، انتخاب توسط کارمندان مجموعه‌سازی که به انتخاب منابع سنتی نیز می‌پردازند انجام می‌شود. برخی از کتابخانه‌های دیجیتالی ترکیبی از رویکردها را بکار می‌برند، در حقیقت این کتابخانه‌ها می‌توانند از مدل ترکیبی استفاده کنند که به ادغام انتخاب توسط هر دو نوع متخصص موضوع و فرمت بپردازند. در رویکرد فرمت - مدار، مجلات الکترونیکی توسط کارمندانی که مهارت الکترونیکی دارند گزینش می‌شوند، در حالی که در رویکرد موضوع - مدار نیازمند آموزش بیشتری هستیم، زیرا متخصصان موضوعی ممکن است هیچ‌گونه مهارت الکترونیکی نداشته باشند.

در انتخاب مجلات الکترونیکی، همانند انتخاب مجلات چاپی از فرایند سه مرحله‌ای شناسایی، ارزیابی و انتخاب استفاده می‌شود. در مرحله نخست، موجودیت عناوین خاص تعیین می‌گردد. در مرحله دوم مفهوم میکرو ارزیابی به جای ماکرو که به معنی ارزیابی یک عنوان خاص به جای کل مجموعه است بکار می‌رود. ارزیابی خصوصیات ذاتی هر عنوان را مشخص می‌سازد. در ارزیابی از فاکتورهای سنتی زیر استفاده می‌گردد:

محتوای موضوعی، زبان انتشار، صحت، جاری بودن، نمایه‌سازی، اعتبار نویسنده، اعضای کمیته ویراستاری، شهرت ناشر، معتبر بودن مجله از نظر داوران متخصص، کیفیت تحقیقاتی کلی و پر مخاطب بودن مجله.

به این معیارهای سنتی معیارهایی در حالت الکترونیکی اضافه می‌گردد که عبارتند از: ارئه مجله بصورت پیوسته، CDROM یا شبکه، فرمت مجله (فرمت اسکی، پست اسکریپت، HTML، یا ...)، سازگاری فنی با تجهیزات کتابخانه، مقدار آموزش مورد نیاز، میزان نگهداری مورد نیاز، جواز دسترسی، رابط کاربر، اعتبار دسترسی، ثبات و آرشیو شدن مجله.

در مرحله آخر، در مورد اینکه آیا آن عنوان برای کتابخانه شما باید انتخاب شود یا خیر تصمیم‌گیری می‌شود. که در این مرحله عواملی نظیر نیازهای کاربران، برنامه درسی مؤسسه، اولویت‌های غیر رسمی مجموعه‌سازی، ملاحظات بودجه، و رابطه آن عنوان با بقیه مواردی که اکنون در مجموعه هستند باید در تصمیم‌گیری انتخاب مورد توجه قرار گیرند.

۲،۴- آرشیوسازی و حفاظت مجلات الکترونیکی

به دلیل زودگذر و ناپایدار بودن فرمت‌های الکترونیکی، مسئله آرشیوسازی و حفاظت دائمی انتشارات الکترونیکی مسئله‌ای بی‌نهایت دشوار است که تاکنون حل نشده است.

همه مجلات الکترونیکی ممکن است از ارزش علمی و تحقیقاتی کافی که آرشیو کردن دائمی آنها را توجیه کند برخوردار نباشد، در نتیجه قسمتی از مسئولیت مدیریت مجموعه مجلات الکترونیکی به تصمیم‌گیری در مورد آرشیو کردن مجلات الکترونیکی بر می‌گردد. نیاز به صرفه‌جویی در فضای ذخیره‌سازی و هزینه، دوام و ارزش علمی مجله و تغییر نیازهای اطلاعاتی کاربران همه مواردی هستند که در بحث آرشیو سازی دخالت دارند.

آرشیوسازی می‌تواند در فرمت‌های متنوعی (کاغذ، دیسک، میکرو فرمت، CDROM، رسانه‌های دیداری یا کامپیوتری) انجام شود.

با انتشار مداوم مجلات الکترونیک بی شک این مورد در آینده با اهمیت تلقی خواهد شد، اکثر معیارهای انتخاب که در بالا مطرح شد می تواند در تصمیم گیری فسخ نیز بکار رود. مسئله عمده در اینجا این است که در صورت فسخ یک مجله الکترونیکی، آیا کتابخانه تمامی آنها را از دست می دهد یا اینکه مجوز دسترسی مجلاتی که برای آنها حق اشتراک پرداخت شده است برای کتابخانه باقی می ماند.

۵- نتیجه گیری :

کتابخانه های دیجیتال محیطهایی هستند که به محققین و پژوهشگران این امکان را می دهند، بدون صرف وقت و هزینه ی زیاد آنها در کنار انبوهی از امکانات مهم تحقیقی ، به منابع مورد نیاز خود دسترسی پیدا نموده و نتایج مطلوب و ارزشمندی را کسب نمایند. بنابراین با توجه به رشد روز افزون چنین مواردی و علاقمند شدن محققین به استفاده از کتابخانه های دیجیتال می بایست اصول معماری خاصی جهت طراحی و پیاده سازی این کتابخانه ها در نظر گرفته شود، همچنین می بایست سرویسهای ویژه ای جهت سهولت کار با این کتابخانه ها در اختیار کاربران قرا گیرد تا بتوانند به راحتی در بین هزاران شی دیجیتال موجود در کتابخانه های دیجیتال موضوعات مورد علاقه خود را به فرمتی قابل استفاده یافته و مورد استفاده قرار دهند. مطلب مهم دیگر در نظر گرفتن مسائل امنیتی و حفاظت از داده ها می باشد. روشهای متعددی در این زمینه وجود دارد که باید به طور جدی تری مورد بررسی قرار گیرند.

6- Reference

- 1- hdl:cnri.dlib/tn95-01 Kahn, Robert and Wilensky, Robert. "A framework for distributed digital object services". May, 1995
- 2- Arms, William Y. (1995). Key Concepts in the Architecture of the Digital Library. D-Lib Magazine Virginia: Corporation for National Research Initiatives Reston
- 3- Key Concepts in the Architecture of the Digital Library
- 4- Arnold, Michael; Schmuker, Martin; Wolthusen, Stephen D. Techniques and Application of Digital Watermarking and Content Protection, (e-book), Artech House Computer Security Series, Artech House, Boston, Mass, 2003.
- 5- Clifton, Chris; Bishop, Matt; Watermarking, Computer Forensics, Risk Management, Legal and Ethical Issues, Course on Computer Security, School of Information Science, University of Pittsburg PA, 2003.
- 6- Doll, Mark W.; Rai, Sanjay; Granado, Jose. Defending the Digital Frontier, (e-book), John Wiley and Son, Hoboken NJ, 2003. European Council of Museums, Archives and Libraries. Technical Guidelines for Digital Cultural Content Creation Program, Working Draft Version 0.01,
- 7- Matsuura, Jeffery H. Managing Intellectual Assets in Digital Age, (e-book), Artech House, Boston MA, 2003.
- 8- Barg, Alexander; Blakely, G.R.; Kabatiansky, Grigory A. Digital Fingerprinting Codes: Problem Statements, Constructions and Identification of Traitors. IEEE Transactions on Information Theory, Vol 49 No. 4, pp 852-865, April 2003.
- 9- Maiwald, Eric; Sieglein, William. Security Planning and Disaster Recovery. (e-bbok), Artech House Computer Security Series, Artech House, Boston MA, 2002.
- 10- Library of Congress. Building a National Strategy for Digital Preservation: Issues in Digital Media Archiving, Council on Library and Information Resources, Washington DC, 2002.
- 11- DeMaio, Harry B. B2B and Beyond: New Business Models Built on Trust, (e-book), John Wiley and Sons, New York NY, 2001.
- 12- Katzenbeisser, Stefan; Petitcolas, Fabian A.P. Information Hiding Techniques for Steganography and Digital Watermarking, (e-book), Artech House Computer Security Series, Artech House, Boston, Mass, 2000.