امنیت و کتابخانه‌های دیجیتال

ترجمه:فرحناز اسماعیل بیگی

1.مقدمه

امنیت یک مسئله مهم در طراحی کتابخانه دیجیتال محسوب می‌شود. ضعف امنیت در کتابخانه‌های دیجیتال، به‌همراه حملات یا دیگر انواع نقایص می‌توانند به دسترسی نامناسب به اطلاعات محرمانه یا از دست رفتن انسجام و یکپارچگی داده‌های ذخیره شده منجر گردد. این‌ها به‌نوبه خود می‌توانند اثر مخربی بر اعتمادناشران یا سایر تولیدکنندگان محتوا داشته باشند و می‌توانند باعث از دست رفتن شهرت یا حتی خسارت اقتصادی مالکان کتابخانه دیجیتال شوند و یا درصورت عدم دسترسی به اطلاعات موردنیاز مبرم، به رنج و درد منجر می‌گردند (تیرواینن[1] 2005).

الزامات امنیتی بسیاری وجود دارند که درنظر گرفته شوند، زیرا انواعی از کاربران مختلف با یک کتابخانه دیجیتال کار و تعامل دارند. هریک از این کاربران، نیازهای امنیتی متفاوتی دارند (چادوری[2]و چادوری، 2003). از این‌رو، یک تولیدکننده محتوای کتابخانه دیجیتال ممکن است نگران حفاظت از حقوق مالکیت معنوی و قوانین استفاده از محتوا باشد، درحالیکه یک کاربر کتابخانه دیجیتال ممکن است نگرانیِ دسترسی معتبر و قابل اعتماد به محتوای ذخیره شده در کتابخانه دیجیتال را داشته باشد. الزامات مبتنی بر این نیازها گاهی اوقات در تناقض هستند که می‌تواند معماری امنیت کتابخانه دیجیتال را پیچیده‌تر نیز بنماید.

طراحی معماری امنیتِ یک کتابخانه دیجیتال باید به‌نحوی باشد که نتوان به‌راحتی یک یا چند ماژول را به سیستمی که قبلاً طراحی شده است، افزود. زیرا ممکن است حفره‌های امنیتی در ماژول‌های موجود وجود داشته باشند و همچنین از این جهت که ممکن است دشواری‌هایی در تلاش برای یکپارچه‌سازی ماژول‌ها به‌وجود آیند. معماری امنیت یک کتابخانه دیجیتال باید به‌نحوی طراحی شود که نگرانی‌های امنیتی به‌صورت کامل و همه-جانبه رفع شوند. یک طراح سیستم امنیت باید کل معماری را مدنظر قرار داده و همه عوامل کاربردی امنیتی را در طراحی یک کتابخانه دیجیتال امن، لحاظ نماید. ماهیت حمله امنیتی ممکن است از لحاظ معماری کتابخانه دیجیتال، متفاوت باشد؛ یک کتابخانه دیجیتال توزیعی نسبت به یک کتابخانه دیجیتال متمرکز، ضعف‌های امنیتی بیشتری دارد.

1. Tyrväinen
2. Chowdhury

حملات امنیتی را می‌توان به حملات فیزیکی و حملات منطقی تقسیم نمود (استالینگز[1] 2006). یک حمله فیزیکی، امنیت سخت‌افزار را نشانه می‌گیرد یعنی جایی‌که کلیدها، قفل‌ها، کارت‌ها و پایش بازدیدکننده مورد استفاده قرار می‌گیرند. یک حمله منطقی با حمله به محتوا یا سیستم کتابخانه دیجیتال همراه است. هدف ما، بررسی حملات منطقی و امنیت نرم‌افزاری کتابخانه‌های دیجیتال است.

2. موضوعات امنیتی مربوط به کتابخانه‌های دیجیتال

طبق مدل مرجع DELOS (کاندلا و همکاران، 2007)، 6 مفهوم اصلی در دنیای کتابخانه دیجیتال وجود دارد: محتوا، کاربر، عاملیت، معماری، کیفیت و سیاست. هریک از این مفاهیم، موضوعات امنیتی مربوط به خودش را دارد که از آنها متأثر می‌شود.

1,2 محتوا

محتوای یک کتابخانه دیجیتال شامل اطلاعاتی است که یک کتابخانه دیجیتال برای کاربران فراهم می‌آورد. برخی از موضوعات امنیتی مربوطه عبارتند از کنترل یکپارچگی و دسترسی. یکپارچگی، مستلزم این است که هر موضوع/ منبعی توسط یک فرد غیرمجاز تغییر نیابد. کنترل دسترسی از دو الزام امنیتی تشکیل می‌شود. الزام اول، احراز هویت است، در جایی‌که کاربر باید وارد سیستم شود و الزام دوم، محرمانه بودن است، به این معنا که محتوای یک موضوع، نباید توسط شخصی به‌غیر از افراد مجاز قابل دسترس باشد. همه کتابخانه‌های دیجیتال رایگان و آزاد نیستند؛ اغلب، محتوا در ازای یک مبلغ خاص در اختیار کاربران کتابخانه قرار می‌گیرد و دسترسی به آن باید به‌منظور حفاظت از محتوا، تحت کنترل قرار گیرد. علاوه بر این، برخی محتواها برای برخی کاربران نامناسب هستند یا به‌صورت هدفمند برای گروه خاصی از کاربران تهیه شده‌اند؛ به همین دلایل، کنترل دسترسی، ضروری است.

حملات منطقی ازجمله هک کردن و دستکاری پیام می‌توانند انسجام و محرمانه بودن محتوا را تحت تأثیر قرار دهند. بهبود دسترسی به اطلاعات در کتابخانه‌های دیجیتال، نگرانی‌های بسیاری را به‌وجود آورده که مدیریت کتابخانه‌های دیجیتال را تحت تأثیر قرار می‌دهد. مدیریت محتوا یا به‌طور اختصاصی‌تر، مدیریت حقوق دیجیتال به حفاظت از محتوا درمقابل حملات امنیتی منطقی و موضوعاتمختلف گفته می‌شود که حقوق مالکیت معنوی را به اعتبار و اصالت مرتبط می‌سازند.

1,1,2 مدیریت حقوق دیجیتال

1. Stallings

مدیریت حقوق دیجیتال (DRM) با رمزگذاری محتوا و مرتبط ساختن آن با یک مجوز دیجیتال، حفاظت از محتوا را تأمین می‌نماید (تیروانن، 2005). این مجوز، کاربر مجاز به مشاهده محتوا را شناسایی کرده، محتوای محصول را فهرست‌بندی نموده و حقوقی که کاربر باید رعایت کند را در یک فرمت قابل قرائت در کامپیوتر با استفاده از زبان بیانی حقوق دیجیتال (DREL) یا زبان نشانه‌گذاری حقوق قابل تعمیم (XrML) وضع می‌کند که محدودیت‌ها و شرایطی را نیز تعیین می‌نمایند.

7 فناوری مورد استفاده برای ارائه DRM وجود دارد (فتشرین[1]و اشمید؛[2] 2003). جدول 1 مؤلفه‌های DRM و فناوری پشتیبان را به‌طور خلاصه نشان می‌دهد.

هریک از این مؤلفه‌ها دربرگیرنده مکانیسم‌های مورد استفاده برای ارائه DRM می‌باشد:

- **رمزنگاری**: تکنیک‌های رمزنگاری ازجمله رمزهای متقارن و نامتقارن که می‌توانند برای کنترل دسترسی مورد استفاده قرار گیرند؛ رمزنگاری کلید عمومی در سیستم‌های پرداخت به‌کار گرفته شده و نحوه و فردی که از محتوا استفاده می‌کند را کنترل می‌نماید.

رمزهای متقارن با استفاده از الگوریتم‌های DES، 3DES، AES و RC4 به استفاده از یک کلید سری مشترک جهت رمزنگاری داده‌ها پیش از ارسال آن نیاز دارند. در انتهای گیرنده، متن رمز با استفاده از همان کلید سری، رمزنگاری می‌شود. رمزهای متقارن به آگاهی فرستنده و گیرنده از کلید مشترک بستگی دارند.

رمزهای نامتقارن از یک جفت کلید برای هر فرستند و گیرنده، استفاده می‌کنند: عمومی و خصوصی. کلیدهای عمومی فرستنده و گیرنده، مشخص می‌باشند، اما کلید خصوصی، سری باقی می‌ماند. اگر رمزنگاری با استفاده از کلید عمومی انجام شود، تنها کلید خصوصی را می‌توان برای رمزنگاری مورد استفاده قرار داد، و برعکس.

- **پسوردها (رمزهای عبور)**: رشته‌های ذخیره شده باید با کاربرانی که دسترسی دارند، مطابقت داشته باشند.
- **واترمارکینگ (نهان‌نگاری)**:اعداد یا تصاویر برای نشان دادن مالکیت، اضافه می‌شوند. پنهان‌نگاری برای پنهان کردن داده‌های درون فایل‌های صوتی، تصویری یا تصاویر به‌کار می‌رود (جانسون[3]و جاجودیا؛[4] 1998). تکنیک‌های مختلف واترمارکینگ، اهداف مختلفی را دنبال می‌کنند؛ برخی از واترمارک‌ها می‌توانند قابل مشاهده باشند، درحالیکه بقیه آنها قابل مشاهده نیستند. برخی واترمارک‌ها برگشت پذیر هستند

1. Fetscherin
2. Schmid
3. Johnson
4. Jajodia

(مینتزر[1]و همکاران، 1997)؛ این وضعیت به استفاده مدنظر از واترمارک و آنچه باید حفاظت شود، بستگی دارد.

- **امضای دیجیتال**: رمزنگاری نامتقارن را می‌توان مورد استفاده قرار داد. همچنین، الگوریتم‌های هش ازجمله MD5 و SHA را می‌توان برای ایجاد امضا به‌کار برد (استالینگز، 2006).
- **اثرانگشت دیجیتال**: اثرانگشت‌های دیجیتال یک تکنیک قدرتمندتر هستند که شامل امضاهای دیجیتال و واترمارکینگ می‌باشند. خالق محتوا، یک نسخهانحصاری از محتوای علامت‌گذاری شده برای هر کاربر ایجاد می‌نماید؛ علامت‌ها خاص کاربر هستند و درنتیجه اثرانگشت نامیده می‌شوند. اگر کاربری به‌صورت غیرقانونی به انتشار محتوا اقدام کند، خالق محتوا می‌تواند از ربات‌های جستجو برای یافتن این نسخه‌های کپی استفاده کند (شانبرگ[2]و کروسکی[3] 2004).
- **سیستم‌های تشخیص کپی**: موتورهای جستجو نیز می‌توانند به تعیین موقعیت چنین آیتم‌های کپی شده کمک نمایند. جستجوگرهای تشخیص دهنده کپی می‌توانند از محتوای دیجیتال نیز حفاظت نمایند.
- **سیستم‌های پرداخت**: کاربران باید اطلاعات شخصی خود را برای پرداخت وجه برای یک محتوا فاش کنند. نصب سیستم‌های پرداخت می‌تواند به حفاظت از محتوای دیجیتال کمک کند.

مؤلفه	فناوری حفاظت
کنترل دسترسی و استفاده	رمزنگاری (برای مثال، متقارن، نامتقارن)، پسوردها
حفاظت از اعتبار و یکپارچگی	واترمارک‌ها، امضاهای دیجیتال، اثرانگشت‌های دیجیتال
شناسایی توسط متاداده	امکان توصیف یک آیتم در طبقات مناسب که محتوای دیجیتال، مالک حقوق و شرایط را پوشش می‌دهند.
سخت‌افزار و نرم‌افزار خاص	شامل همه سخت‌افزارها و نرم‌افزارهای مورد استفاده توسط دستگاه نهایی است که از طریق آن، محتوای دیجیتال نمایش داده شده، مشاهده شده یا چاپ می‌شود.
سیستم‌های تشخیص کپی	موتورهای جستجو که شبکه را برای یافتن کپی‌های غیرقانونی و استفاده از واترمارکینگ جستجو می‌کنند.
سیستم‌های پرداخت	می‌توانند به‌عنوان نوع خاصی از فناوری حفاظت درنظر گرفته شوند، زیرا مستلزم ثبت‌نام کاربر یا احراز هویت کارت اعتباری است که آن نیز به یک رابطه اعتماد بین تولیدکننده محتوا و مشتری نیاز دارد.
سیستم‌های تجارت الکترونیکی یکپارچه	DRMS باید شامل سیستم‌هایی باشد که پشتیبان مذاکره قرارداد، اطلاعات حسابداری و قوانین کاربرد هستند.

1. Mintzer
2. Schonberg
3. Kirovski

هیچ مکانیسم استانداردی برای ارائه DRM وجود ندارد، بیشتر به علت کمبود مقررات در این زمینه (چادوری و چادوری، 2003)، با این حال، سیستم‌ها و پروتکل‌های مختلفی وجود دارند که برای ارائه سیاست‌های استفاده منصفانه از مدیریت و پشتیبانی محتوا معرفی می‌شوند.

بین امنیت و عملکرد باید یکی را قربانی نمود. نادیم[1]و جواد از یک دستگاه پنتیوم 4 2/4 گیگاهرتزی با سیستم عامل مایکروسافت ویندوز XP استفاده نموده و 20527 بایت را به 2323398 بایت داده با استفاده از DES، 3DES و AES رمزنگاری نمودند. برای 20527 بایت داده، 2 ثانیه زمان نیاز است تا با استفاده از الگوریتم DES رمزنگاری انجام شود و 4 ثانیه برای رمزنگاری با استفاده از الگوریتم AES زمان نیاز است (نادیم و جواد، 2005). می‌توان مشاهده نمود که هرچه الگوریتم رمزنگاری پیچیده‌تر باشد، رمزنگاری داده‌ها بیشتر به‌طول می-انجامد. در مطالعه دیگر، رمزنگاری داده‌ها با الگوریتم RSA با استفاده از یک کلید با اندازه 1024، 0/08 میلی-ثانیه به ازای اجرا بر یک پردازش‌گر اینتل کور 2 1/83 گیگاهرتز تحت ویندوز ویستا در حالت 32 بیت زمان صرف نمود، درحالیکه با استفاده از یک کلید با اندازه 2048، این زمان به 0/16 میلی‌ثانیه به ازای اجرا افزایش می‌یابد (دای،[2] 2009).

2,2 کاربر

کاربر در یک کتابخانه دیجیتال، به «عاملان مختلفی (انسان یا دستگاه) گفته می‌شود که مجاز به تعامل با کتابخانه‌های دیجیتال می‌باشند» (کاندلا[3]و همکاران، 2007).کتابخانه‌های دیجیتال، عاملان مختلف را با اطلاعاتی که در اختیار دارند به یکدیگر متصل نموده و به کاربران امکان استفاده از اطلاعات قدیمی یا تولید اطلاعات جدید را می‌دهند. مسائل امنیتی مرتبط با کاربران یک کتابخانه دیجیتال با مسائل محتوایی فوق‌الذکر تلاقی می‌کنند. یک مسئله امنیتی منطقی مهم مرتبط با کاربران و محتوا، کنترل دسترسی است. الزامات مختلف کنترل دسترسی، برای سیستم‌های توزیع شده تعیین می‌شوند (تولون[4]و همکاران، 2005). تا هم از محرمانه بودن و هم از احراز هویت اطمینان حاصل شود:

- کنترل دسترسی باید به‌کار گرفته شده و در سطح پلتفرم توزیع یافته اعمال شود، بنابراین باید مقیاس-پذیر بوده و در سطوح مختلف دانه‌بندی، قابل دسترس باشد.

1. Nadeem
2. Dai
3. Candela
4. Tolone

- مدل‌های کنترل دسترسی باید امکان تعریف متفاوتی از حقوق دسترسی را بسته به اطلاعات مختلف فراهم آورده و باید در مواردی که تغییرات سیاست‌ها به‌راحتی صورت گرفته و مدیریت آنها آسان است، دینامیک باشند.
- «مدل‌های کنترل دسترسی باید مشخصات سطح بالای حقوق دسترسی را محقق نمایند». (تولون و همکاران، 2005).

کاربران کتابخانه دیجیتال ممکن است پیش از اینکه بتوانند به محتوا دسترسی پیدا کنند نیاز به احراز هویت داشته باشند. شناسایی سراسری یا فراگیر ممکن است کافی نباشد. ارائه دهنده خدماتی که محتوا را براساس معیارهای غیرهویتی مانند سن ارائه می‌دهند، از شناسایی سراسری بهره‌مند نخواهد شد، زیرا هیچ راهی برای تأیید اطلاعات شخصی کاربر احراز هویت شده وجود ندارد. نام‌های کاربری و رمزهای عبور، روش‌های کارآمدی برای احراز هویت نیستند.

یکی از پر کاربردترین پروتکل‌های احراز هویت، کربرس[1]است. این پروتکل (نیومن[2]و تسو[3] 1994) یک مدل کاربر- سرور است که ارتباط با سرورهای روی یک شبکه محلی را ایمن می‌کند. این پروتکل که در MIT در دهه 1980 برای تأمین امنیت در سراسر یک شبکه بزرگ دانشگاهی توسعه یافته است، براساس پروتکل نیدام-شرودر[4]است و اکنون به‌صورت استاندارد درآمده و در بسیاری از سیستم‌های عامل مانند UNIX، Linux،ویندوز 2000، NT، XP و غیره وجود دارد.

کربرس به‌عنوان یک پروتکل احراز هویت در مواردی که حمله‌کنندگان ترافیک شبکه را برای متوقف نمودن رمزهای عبور نظارت می‌کنند، مورد استفاده قرار می‌گیرد. این پروتکل، ارتباطات را ایمن ساخته و یک ثبت نام منفرد و احراز هویت دوطرفه ایجاد می‌نماید و یک رمزعبور کاربری را به‌وضوح بر روی یک شبکه ناایمن نمی-فرستد.

راه‌حل دیگر مناسب برای کتابخانه‌های دیجیتال (وینسلت[5]و همکاران، 1997)، اطلاعات مربوط به یک فرد را با استفاده از اعتبارنامه‌ها ارائه می‌دهد. اعتبارنامه‌ها «آیتم‌های مختصری هستند که شامل جملاتی می‌باشند که دانش یا اطلاعات را از یک زمینه مشخص، بیان می‌نمایند». اعتبارنامه‌ها، اطلاعات مستقیمی درمورد یک

1. Kerberos
2. Neuman
3. Ts‘o
4. Needham-Schroeder
5. Winslett

مشتری و ویژگی‌های آنها، مشخص می‌نمایند، اعتبارنامه‌ها محیط محلی و زمینه‌ای که درخواست‌ها از آن نشأت می‌گیرند را شرح می‌دهند (چینگ[1]و همکاران، 1996).

اعتبارنامه‌های دیجیتال را می‌توان به‌عنوان ابزاری برای احراز هویت در ارائه کنترل دسترسی DL استفاده کرد (وینسلت و همکاران، 1997). از دو عامل می‌توان برای کمک به مدیریت استفاده کرد: یک دستیار امنیت شخصی و یک دستیار امنیت سرور، برای مدیریت اعتبارنامه‌های دیجیتال با استفاده از یک مدل مشتری/ سرور. سرور باید مشتری را از اعتبارنامه‌های موردنیاز برای درخواست فعلی آگاه نماید.سپس مشتری اعتبارنامه خود را برای احراز هویت ارسال می‌کند. مشتری باید به سرور کمی اعتماد داشته باشد تا اعتبارنامه خود رابدهد، که این امر باعث ایجاد مسائل مربوط به حریم خصوصی می‌شود.

دستیار امنیت شخصی برای به‌دست آوردن اعتبارنامه از طرف مشتری، ذخیره اعتبارنامه‌ها، تجزیه و تفسیر اعتبارنامه‌های موردنیازو مدیریت سیاست‌های پذیرش مورد استفاده قرار می‌گیرد (وینسلت و همکاران ، 1997). یک دستیار امنیت سرور برای تعیین خط‌مشی‌های پذیرش اعتبارنامه و کاربرد آنها در دسترس است.

بین انعطاف‌پذیری و امنیت باید انتخاب انجام گیرد که باید هنگام انتخاب مدل کنترل دسترسی در نظر گرفته شود ، همان‌طور که در زیر بحث شده است.

1,2,2 مدل ماتریکس دسترسی

این مدل مفهومی، حقوقی را که هر موضوع برای هر آیتم در اختیار دارد، مشخص می‌کند (تولون و همکاران، 2005). اقدامات مربوط به آیتم‌ها براساس حقوق دسترسی مشخص شده، مجاز یا رد می‌شوند.2 اجرای AMM وجود دارد:

- یک فهرست کنترل دسترسی، نقشه‌برداریِ مستقیمی از هر آیتم که افراد، مجاز به دسترسی به آنها هستند و حقوق استفاده از آنها (مالک، خواندن یا نوشتن) را فراهم می‌کند.
- یک فهرست قابلیت،آیتم‌هایی را که هر فرد، مجاز به دسترسی به آنهاست و حقوق استفاده را تعریف می‌نماید.

فهرست‌های کنترل دسترسی و فهرست‌های قابلیت برای سیستم‌های توزیع یافته مناسب نیستند. محدودیت‌های آنها منجر به مشکلات متعددی می‌شود (نگاراج[2] 2001). ACL بیان‌پذیری محدود سیاست‌ها را فراهم می‌کند. هرگونه تغییر در خط‌مشی‌ها، در سیستم یا برنامه‌های کاربردی گسترش خواهد یافت. احراز هویت در

1. Ching
2Nagaraj

سیستمی که فقط از ACL استفاده می‌کند، یک مشکل است، زیرا استفاده از نام کاربری و رمز عبور در یک سیستم توزیع یافته، عملی نیست. در یک سیستم توزیع یافته، مدیریت سیستم باید با تفویض اختیار، غیرمتمرکز شود تا سربار کاهش یابد. مالک آیتم، یک خط‌مشی را در ACL مشخص می‌کند. اگر خط‌مشی کلی توسط نهادی بالاتر از مالک آیتم مشخص شود، ممکن است در حقوق دسترسی تعارضاتی رخ دهد. تعداد نهادهای اداری در یک سیستم توزیع یافته می‌تواند بسیار زیاد باشد. ممکن است همه مدیران بین خودشان اعتماد نداشته باشند که این امر به تعریف سیاست‌های نادرست منجر می‌گردد. به‌عنوان مثال، مدیر A ممکن است به B اعتماد داشته باشد اما به C اعتماد نکند، با این حال، B ممکن استب بهC اعتماد داشته باشد. اگر A برای B خط‌مشی تعریف کند، به‌طور ضمنی برای C قابل اجرا خواهد بود، و باعث ایجاد مشکل می‌شود.

2,2,2 کنترل دسترسی مبتنی بر نقش

کنترل دسترسی مبتنی بر نقش شامل سیاست‌هایی است که دسترسی به اطلاعات را براساس فعالیت‌هایی که کاربران انجام می‌دهند تنظیم می‌کنند. چنین سیاست‌هایی مستلزم تعریف نقش‌ها در سیستم می‌باشند: «مجموعه‌ای از اقدامات و مسئولیت‌های مربوط به یک فعالیت کاری خاص» (ساندو[1]و ساماراتی[2] 1994). مجوزها به‌جای کاربران به نقش‌ها اختصاص می‌یابند. تعیین مجوز کاربر شامل 2 مرحله است: اول، اختصاص دادن یک نقش به هر کاربر، دوم، تعریف کنترل دسترسی که نقش برای آیتم‌های خاصی دارد.

مدیریت RBAC نسبت به ACL، آسان‌تر و قابل تعمیم‌تر است. با این حال، RBAC به‌طور انعطاف‌پذیر به محدودیت‌ها نمی‌پردازد، مثلاً در جایی‌که یک کاربر با نقش خاص ممکن است مجوز خاصی برای یک آیتم داشته باشد. یک نمونه از معماری RBAC که به محدودیت‌های کلیدی می‌پردازد،OASIS (بیکن[3]و همکاران، 2003) برای استفاده در سیستم‌های توزیع یافتهمی‌باشد. مدیریت نقش در OASIS غیرمتمرکز و خاص خدمت می‌باشد. OASIS با یک میان‌افزار مبتنی بر رویداد تلفیق می‌شودکه هرگونه تغییر در محیط را به برنامه‌ها اطلاع می‌دهد. نقش‌ها توسط برنامه‌ها و سرویس‌ها برای تعریف نقش‌های مشتری خود و اعمال سیاست‌ها برای فعال-سازی نقش و فراخوانی خدمت در هر نشست، پارامتری می‌شوند. گواهینامه‌های عضویت در نقش (RMC)با ورود موفقیت آمیز به هر کاربر داده می‌شوند تا به‌عنوان اعتبارنامه برای فعال‌سازی سایر نقش‌ها استفاده شوند (بیکن و همکاران، 2003)

RBAC برای استفاده در کتابخانه‌های دیجیتال مناسب است، زیرا از نقش‌های مختلف معماری غیرمتمرکز پشتیبانی می‌کند، با این وجود، RBAC اجازه تعریف نقش‌های مختلف در یک گروه مشترک را نمی‌دهد.

1. Sandhu
2. Samarati
3. Bacon

3,2,2 کنترل دسترسی مبتنی بر وظیفه

مدل کنترل دسترسی مبتنی بر وظیفه با فراهم آوردن امکان تعریف حوزه‌ها براساس اطلاعات متنی مبتنی بر وظیفه، کنترل دسترسی موضوع / آیتم را گسترش می‌دهد (تولون و همکاران، 2005). مراحل موردنیاز برای انجام وظیفه، برای تعریف کنترل دسترسی استفاده می‌شود؛ مراحل مربوط به یک حالت محافظتی شامل مجموعه‌ای از مجوزها برای هر حالت است، که متناسب با وظیفه، تغییر می‌کند. TBAC از مدیریت پویای مجوزها استفاده می‌کند.

سیستم‌های TBAC به تعریف زمینه‌های مرتبط با فعالیت‌ها، وظایف یا پیشرفت گردش کار محدود می‌شوند.از آنجا که TBACبا ثبتاستفاده و اعتبار مجوزها اجرا می‌شود، بنابراین، به یک ماژول کنترل دسترسی مرکزی برای مدیریت فعال‌سازی و غیرفعال‌سازی مجوزها به روشی به‌هنگامنیاز دارد.

4,2,2 کنترل دسترسی مبتنی بر تیم

RBAC به مواردی که اعضای گروه با نقش‌های مختلف می‌خواهند در یک گروه واحد انجام دهند، نمی-پردازند.مدل TMAC همکاری با زمینه کاربر و زمینه آیتم را تعریف می کند. «زمینه کاربر، راهی برای شناسایی کاربران خاص است که نقشی را در یک تیم در هر لحظه خاص از زمان ایفاء می‌کنند، فراهم می‌آورد» (تولون و همکاران، 2005)، درحالیکه زمینه آیتم، آیتم‌ها و اهداف موردنیاز را تعریف می‌کند.

TMACمزایای RBAC را به‌همراه توانایی تعیین کنترل دقیق بر کاربران و نمونه‌های شیء ارائه می‌دهد. یک ساختار داده کنترل دسترسی مقیاس‌پذیر را می‌توان با مجموعه‌های بزرگ، استفاده نمودکه مفاهیم کنترل دسترسی مبتنی بر تیم را اعمال نموده، بیشتر بر ساختار داده کنترل دسترسی تمرکز داشته و یک چارچوب کنترل دسترسی به نام روش کنترل دسترسی به اسناد (DACM) را به‌همراه سیستم ذخیره‌سازی اسناد (DocSS) به‌کار می‌گیرد (گلادنی، 1997). DACM امکان مدیریت غیرمتمرکز امتیازات، تعریف مجموعه قوانین مختلف برای کنترل یک مجموعه واحد و الگوهای مختلف تفویض اختیار به‌صورت مدل‌هایی را فراهم می‌آورد.

سیاست‌های کنونی، کنترل دسترسی آیتم از آرایه‌ای از قوانین برای ثبت امتیازاتی که هر موضوع به هر شی می‌دهد، استفاده می‌کند. مدیریت این امر در مجموعه داده‌های کلان موجود در کتابخانه‌های دیجیتال، غیرعملی است. DACM این مشکل را با یافتن تقارن‌هایی در یک تابع مجوز، حل می‌کند تا بیان مختصر و بدون از دست دادن تمایزهای مهم را فراهم کند.

5,2,2 کنترل دسترسی مبتنی بر محتوا

رویکرد دیگر برای مدل‌های کنترل دسترسی شامل تعریف مدل‌هایی مطابق با محتوا می‌باشد. این روش در کتابخانه‌های دیجیتال و سیستم‌های توزیع یافته قابل اجرا است (آدام[1]و همکاران، 2002)، در شرایطی که حقوق دسترسی کاربر، پویا است و ممکن است با هر بار ورود به سیستم، تغییر کند. سیاست های کنترل دسترسی مبتنی بر محتوا برای کتابخانه‌های دیجیتال و سیستم‌های توزیع یافته بسیار مناسب هستند. تحقیقات اخیر، مدل‌های مختلفی را پیشنهاد نموده‌اند؛ که بیشتر آنها از اعتبارنامه دیجیتال برای احراز هویت استفاده می-کنند، اما در تعریف/ ذخیره‌سازی خط‌مشی متفاوت هستند.

یک مدل مهم کنترل دسترسی مبتنی بر محتوا (فراری[2]و همکاران، 2002)، یک سیستم کنترل دسترسی مبتنی بر محتوا، سیستم مجوزدهی کتابخانه دیجیتال را معرفی می‌کند که از مدل مجوزدهی کتابخانه دیجیتال(DLAM) استفاده می‌کند.موضوعات، اشیاء و مجموعه امتیازات نمی‌توانند برای تعریف خط‌مشی‌ها در کتابخانه‌های دیجیتال مورد استفاده قرار گیرند، بیشتر به این دلیل که DL ها با مجموعه‌های بزرگ داده‌ها و موضوعات، پویا هستند. این امر، سیاست‌های کنترل دسترسی را براساس صلاحیت‌ها و ویژگی‌های موضوع تعریف می‌کند. DLAM، ابزاری را برای تعیین صلاحیت‌ها و مشخصات افراد فراهم می‌کند. این از کنترل دسترسی وابسته و مستقل از محتوا استفاده می‌کند و تعریف سیاست‌ها را با جزئیات مختلف امکان‌پذیر می‌کند.

3,2 عاملیت

مفهوم عاملیت دربرگیرنده خدماتی است که یک کتابخانه دیجیتال به کاربران خود ارائه می‌دهد (گونکالوز[3]و همکاران، 2008). حداقل توابع کتابخانه دیجیتال شامل افزودن آیتم‌های جدید به کتابخانه یا جستجو و مرور کتابخانه و سایر توابع مربوط به مدیریت DL می‌باشند.یک حمله امنیتی که می‌تواند بر عاملیت کتابخانه دیجیتال تأثیر بگذارد، حمله عدم پذیرش خدمات است که می‌تواند بر عملکرد سیستم تأثیر بگذارد و از دسترسی کاربران به سیستم جلوگیری کند.

4,2 معماری

کتابخانه‌های دیجیتال، اشکال پیچیده ای از سیستم‌های اطلاعاتی هستند که در کتابخانه‌های مختلف با یکدیگر قابل تطبیق هستند و بنابراین به یک چارچوب معماری نیاز دارند تا محتوا و عاملیت را روی مؤلفه‌های نرم‌افزاری و سخت‌افزاری نقشه‌برداری کنند (کاندلا و همکاران، 2007). مدل‌های مختلفی برای معماری وجود دارند، به-عنوان مثال،مشتری-سرور، نظیر به نظیر و توزیع یافته. همه اینها نیاز به محافظت از کانال‌های ارتباطی بین دو

1Adam
2Ferrari
3Gonçalves

طرف دارند، جایی‌که ممکن است داده‌های حساس منتقل شوند (کوهل[4] و همکاران، 1998). ایمن‌سازی ارتباطات بسته به معماری سیستم، به لایه‌های مختلفی بستگی دارد: اینترنت، انتقال یا لایه برنامه.

مدل توزیع یافته، مقیاس‌پذیر و انعطاف‌پذیر است. هنگام ساخت کتابخانه دیجیتال با تغییر محتوا از منابع مختلف، مفید است و پتانسیل افزایش قابلیت اطمینان را دارد. الزامات امنیتی برای یک کتابخانه دیجیتالی توزیع یافته، چالش‌برانگیز است، زیرا محتوا و عملیات غیرمتمرکز هستند. تلورانسنقص و بازیابی خطا، مواردی هستند که بر یک سیستم توزیع شده تأثیر می‌گذارند. برای افزایش قابلیت دسترسی سیستم از تکرار استفاده می‌شود. درحالی‌که این روش مشکلات مربوط به حملات عدم پذیرش سرویس را حل می‌کند، اما محافظت از محتوا را پیچیده می‌کند، زیرا تکرار محتوا وجود دارد.

مدل مشتری- سرور، مشکلات امنیتی مشابه مدل توزیع یافته عمومی را ندارد، با این حال،ضعف امنیتی بزرگی را به‌همراه دارد، سرور، تنها یک نقطه شکست خاص است. حملات بیشتر از اینکه در چندین نسخه از یک مدل توزیع یافته قرار بگیرند، روی یک سرور متمرکز می‌شوند.

5,2 کیفیت

محتوا و رفتار یک کتابخانه دیجیتال با پارامترهای کیفیت، مشخص و ارزیابی می‌شود. کیفیت (گونکالوز و همکاران، 2007) مفهومی است که نه‌تنها برای طبقه‌بندی عاملیت و محتوا استفاده می‌شود، بلکه از اقلام نیز استفاده می‌شود.. برخی از پارامترها به طور خودبه خود اندازه‌گیری می‌شوند و ذهنی هستند در حالی‌که برخی دیگر به‌صورت موضوعی در نظر گرفته می‌شوند؛ برخی از طریق ارزیابی کاربر اندازه گیری می‌شوند.

6,2 خط‌مشی

خط‌مشی، مفهومی است که مقررات و شرایط مختلف حاکم بر تعامل بین کتابخانه دیجیتال و کاربران را نشان می‌دهد. خط‌مشی‌ها از هر دو تعامل خارجی و ذاتی (کاندلا و همکاران، 2007) و تعریف و اصلاح آنها حمایت می‌کنند. نمونه‌هایی از مسائل امنیتی مربوط به سیاست‌ها عبارتند از ارائه مدیریت حقوق دیجیتال، حریم خصوصی و محرمانه بودن محتوا و کاربران، تعریف رفتار کاربر و تحویل مجموعه.

3. خلاصه

کتابخانه‌های دیجیتال باید امن باشند. امنیت کیفیت مهمی است و همانطور که در بالا با استفاده از تعیین مشخصه‌های DL مدل مرجع DELOS نشان داده شده استبر همه جنبه‌ها تأثیر می‌گذارد (کاندلا و همکاران،

4. Kohl

2007). ما همچنین می‌توانیم این نکته را با استفاده از چارچوب دیگری برای DL ها خلاصه کرده و شرح دهیم (گونکالوز و همکاران، 2004).

چارچوب 5S از جوامع و نیازهای آنها پشتیبانی کرده، تمام جنبه‌های فوق‌الذکر درباره کاربران و خط‌مشی‌های مربوطه و همچنین کیفیت را پوشش می‌دهد (گونکالوز و همکاران، 2007). از آنجا که جوامع شاملعاملان نرم-افزاری، نمایندگان، اجزا، ماژول ها و غیره می‌شوند، این نیز دربرگیرنده موارد معماری مرتبط است. از این‌رو، امنیت باتوجه به جوامع،موضوعاتی مانند مشتری/ سرور، تجارت، هویت، نظیر به نظیر، حریم خصوصی، حقوق، نقش‌ها، تیم‌ها و اعتماد را تحت پوشش قرار می‌دهد.

سناریوها، عملکردها، عملیات، الزامات، خدمات و وظایف را پوشش می‌دهند. نمونه‌هایی از این دست (کونگالوزو و همکاران، 2008) عبارتند از دسترسی، کنترل دسترسی، احراز هویت، مرور، کپی، حملات عدم پذیرش سرویس، رمزنگاری، پرداخت، بازیابی، جستجو، استفاده و واترمارکینگ.

فضاها، جنبه‌های توزیع یافته و همچنین نمایش‌های مربوط به فضاهای یک‌بعدی، دوبعدی، سه‌بعدی و ابعاد بالاتر را پوشش می‌دهند که شامل ویژگی‌ها، اندازه‌ها، متریک، احتمالات، بردار و فضاهای توپولوژیک است که در سرتاسر سیستم‌های کامپیوتری و انسانی استفاده می‌شوند.

ساختارها انواع سازمان‌ها را پوشش می‌دهند، از جمله ساختارهای داده و پایگاه داده، به‌همراه فهرست‌هد (به-عنوان مثال، کنترل یا قابلیت دسترسی)، نمودارها و شبکه‌ها ساختارها روی سایر ساخت‌ها در چارچوب 5S به-ویژه در جریان‌ها، قرار می‌گیرند. بنابراین، اسناد، جریان‌های ساختاربندی شده هستند، درحالی‌که پروتکل‌ها شامل سناریوهایی هستند که برای جریان‌های ارتباطی ساختاربندی شده اعمال می‌شوند. ساختارها و جریان‌ها انواع محتوا و بسیاری از مسائل امنیتی مربوط به آن را پوشش می‌دهند ازجمله مدیریت حقوق دیجیتال، اثرانگشت‌ها و واترمارک‌ها.

بدیهی است که پشتیبانی امنیتی DL می‌تواند پیچیده باشد، اما بحث فوق باید به خوانندگان کمک کند تا تفکر خود را سازماندهی کنند و اطمینان حاصل کنند که سیستم‌های DL الزامات امنیتی را محقق می‌سازند.