فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال هفتم، شماره‌های ۲۳ و ۲۴، بهار و تابستان ۱۳۹۴
صص: ۸۸- ۷۹

مدیریت کلید در سیستم‌های مدیریت حقوق دیجیتال در حالت برون‌خطی

*نفیسه شفیعی **مهدی شجری
*کارشناسی ارشد، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران
** استادیار، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران

تاریخ دریافت: ۱۳۹۳/۱۰/۰۱ تاریخ پذیرش: ۳/ ۱۳۹۴/۰۵

چکیده

با توجه به گسترش کاربرد سیستم‌های مدیریت حقوق دیجیتال، بکارگیری روش‌هایی همانند رمزنگاری و نهان‌نگاری اگرچه دارای برتری‌هایی است، ولیکن تامین‌کننده‌ی نیازمندی‌های سیستم‌های یاد شده به عنوان مسئول توزیع امن محتوای دیجیتال نمی‌باشند. در همین راستا نیاز به یک روش جایگزین و یا ترکیبی به منظور حفاظت از محتوای دیجیتالی از مرحله‌ی تولید تا انتقال و ذخیره‌ی داده‌ها در سیستم‌های مدیریت حقوق دیجیتال امری انکارناپذیر است. در این مقاله، ما مدلی برای بهبود عملکرد سیستم‌های مدیریت حقوق دیجیتال پیشنهاد کرده‌ایم، که اساس کار آن مبتنی بر رمزنگاری چند بخشی بوده و نه تنها بر انتشار و پخش اسناد نظارت و کنترل می‌کند، بلکه با بکارگیری داده‌های متمایز و یکتا در تولید کلید، از کپی‌برداری نیز به طور موثر جلوگیری می‌نماید. وجه تمایز اصلی رویکرد پیشنهادی با سایر روش‌های به کارگرفته شده در این حوزه، استفاده از تکنیک مبهم‌سازی به منظور محافظت از الگوریتم تولید کلید در برابر حملات مهندسی معکوس می‌باشد. سیستم پیشنهادی در مقایسه با سیستم‌های مطرح در زمینه‌ی مدیریت حقوق دیجیتال معیارهای امنیتی بیشتری را پوشش می‌دهد.

واژه‌های کلیدی: مدیریت حقوق دیجیتال، رمزنگاری، مدیریت کلید، کپی‌برداری.

۱. مقدمه

در طی سالیان اخیر با رشد چشمگیر و استفاده‌ی گسترده از اینترنت و فناوری اطلاعات، امکان ایجاد تغییر و کپی‌برداری در محصولات دیجیتال برای افراد فراهم شده‌است. انتشار محتوای دیجیتال در فضای اینترنت از یک طرف نیازمند حفظ حریم خصوصی است، و از طرف دیگر تهدیدی بزرگ برای مؤلفان محسوب می‌شود. علاوه بر این، از دست رفتن حریم خصوصی پس از اجرای یک سیستم مبتنی بر مدیریت حقوق دیجیتال مشکلی بحرانی است، چراکه تمایل کاربران به اتخاذ این دست فناوری‌ها بسیار کند است.

بنابراین محافظت از محتوای دیجیتال در برابر کپی‌برداری در تبادلات اینترنتی موضوعی است که بایستی مورد توجه قرارگیرد. در همین راستا، مدیریت حقوق دیجیتال به عنوان راه‌حلی مانع از توزیع و تکثیر غیرقانونی داده‌های دیجیتال می‌شود[۱].

بکارگیری تکنیک‌های رمزنگاری در سیستم‌های مدیریت حقوق دیجیتال تا مدت‌ها به عنوان راه‌حل اصلی برای جلوگیری از کپی‌برداری غیرمجاز محصولات دیجیتال محسوب می‌شدند.

نویسندهٔ عهده‌دار مکاتبات: مهدی شجری mshajari@aut.ac.ir

اگرچه رمزنگاری از دسترسی کاربران غیرمجاز به فایل‌های رمزشده جلوگیری، و امکان مشاهده و استفاده از آنها را تا حدی مشکل می‌نماید، با این حال تنها به محافظت از داده-های دیجیتال در مرحلهٔ انتقال می‌پردازد. به عبارت دیگر هنگامیکه محتوای دیجیتال برای نخستین بار رمزگشایی می‌شود، پس از آن هیچ کنترل و نظارتی بر روی داده‌ها صورت نمی‌گیرد. در حال حاضر با توجه به فراگیر شدن مفهوم جامع مدیریت حقوق دیجیتال، توجه به جنبه‌های دیگر محتوای دیجیتال علاوه بر انتقال، از جمله تولید، محافظت، مشاهده، استفاده، ... امری مهم و حیاتی است[۲].

از دیگر روش‌های متداول در سیستم‌های مدیریت حقوق دیجیتال، نهان‌نگاری است [۴،۳]. نهان نگاری، علم پنهان سازی اطلاعات مهم داخل اطلاعاتی دیگر است، و این کار باید به گونه‌ای صورت گیرد که اطلاعات میزبان از بین نرود، و همچنین کسی نتواند از وجود اطلاعات مخفی مطلع شود. این روش به عنوان عاملی بازدارنده در برابر کپی‌برداری و ابزاری برای شناسایی محتوای دیجیتال کپی شده و مخدوش شده، مزیت‌هایی برای صاحبان حقوق فراهم می-نماید. با توجه به اینکه محتواهای دیجیتال در سمت کاربران نهایی در مقابل حملات آسیب‌پذیر هستند، مالک اثر می‌تواند با استفاده از نشانه‌های موجود در نهان‌نگاری به شناسایی منبع اصلی بپردازد، و با ردیابی خود مانع از تولید و توزیع و یا ذخیره‌سازی نسخه‌های غیرقانونی شود، با این وجود نمی‌تواند هیچ اقدام مؤثری برای جلوگیری از کپی‌برداری انجام دهد. به عبارت دیگر تنها پس از کپی‌برداری محتوای دیجیتال می‌تواند به تعقیب داده‌های خود بپردازد، و این از جمله محدودیت‌ها و ضعف‌های اصلی نهان‌نگاری به حساب می‌آید.

در نهایت می‌توان چنین گفت که با وجود ارائه‌ی رویکردهای متفاوتی[۶،۵] در زمینه‌ی سیستم‌های مدیریت حقوق دیجیتال تاکنون هیچ معماری استانداردی در این زمینه وجود ندارد. بنابراین، نیاز به یک روش جایگزین و یا ترکیبی به منظور حفاظت از محتوای دیجیتالی از مرحله‌ی تولید تا انتقال و ذخیره‌ی داده‌ها در سیستم‌های مدیریت حقوق دیجیتال امری انکارناپذیر است. صرف استفاده از روش‌هایی همانند رمزنگاری و نهان‌نگاری اگرچه دارای برتری‌هایی است، ولی برای برآورده کردن ضروریات سیستم‌های مدیریت حقوق دیجیتال کافی نمی‌باشد.

در این مقاله، ابتدا به مبانی مفهوم مدیریت حقوق دیجیتال می‌پردازیم، و در بخش سوم پیشینه‌ی پژوهش و کارهای انجام شده در این زمینه را بررسی می‌نماییم. سپس در بخش چهارم سیستم پیشنهادی خود را که شامل رویکردی مبتنی بر رمزنگاری برای مدیریت کلید می‌باشد، معرفی می‌کنیم. در بخش پنجم به ارزیابی مدل پیشنهادی پرداخته و نتایج آن را با دیگر سیستم‌های موجود مقایسه می‌کنیم. در نهایت در بخش ششم جمع‌بندی و نتیجه‌گیری ارائه می‌شود.

۲. مدیریت حقوق دیجیتال[1]

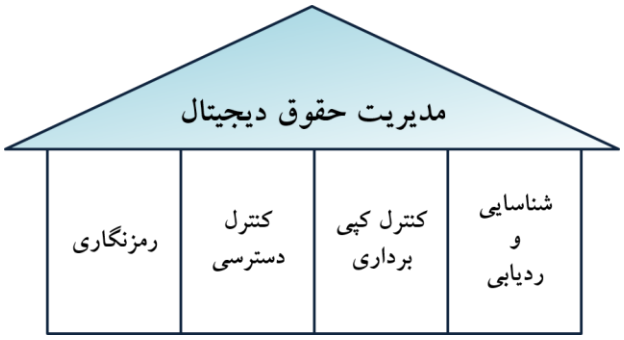
به طور معمول، مدیریت حقوق دیجیتال در رسانه‌های مختلفی کاربرد دارد، اما اغلب در فایل‌های موسیقی، فیلم‌ها، ویدئوها و کتاب‌های الکترونیکی دیده می‌شود.

مدیریت حقوق دیجیتال مجموعه فناوری‌هایی است که موظف به نظارت بر دستیابی به دارایی‌های دیجیتال می‌باشد.

این فناوری‌ها همواره در تلاش هستند، تا قابلیت کنترل را به فروشندگان محصولات با محتوای دیجیتالی بدهند. همانطور که در شکل ۱.۲ مشاهده می‌کنید، کلیه‌ی سیستم‌های مدیریت حقوق دیجیتال دارای توابع و ماژول‌های زیر می‌باشند:

- رمزنگاری
- رمز کردن محتوای دیجیتال
- مدیریت کلید رمزگشایی
- تعریف کنترل دسترسی در چهارچوب استفاده‌ی آسان
- شناسایی و ردیابی محتوای دیجیتال
- کنترل کپی‌برداری

1. Digital Right Management(DRM)



شکل ۱.۲ – اجزای اصلی مدیریت حقوق دیجیتال

صحت و اعتبار و توزیع امن و مطمئن محتوای دیجیتال از جمله مهم‌ترین اهداف مدیریت حقوق دیجیتال محسوب می‌شوند. برای مثال، یک کتاب الکترونیکی را در نظر بگیرید. با وجود اینکه برخی از کتاب‌ها با بکارگیری تکنیک‌های رمزنگاری در فضای مجازی انتشار می‌یابند. اما اگر گیرنده بتواند کتاب را دریک فرمت رمز نشده ذخیره نماید، امکان توزیع غیرقانونی آن در وسعت زیاد وجود خواهد داشت. این ترس باعث شده است که ناشران تا حدی از انتشار کتاب‌های دیجیتال خود به صورت الکترونیک صرف نظر نمایند. در نتیجه بدون وجود یک سیستم مدیریت حقوق دیجیتال قوی، ناشران نمی‌توانند به آن تکیه کنند[۷].

از دیدگاهی دیگر مدیریت حقوق دیجیتال امکان تجارت دیجیتالی را فراهم می‌کند. مدیریت حقوق دیجیتال امتیازات مهمی را فراهم می‌کند که این امتیازات انجام تجارت دیجیتالی را ممکن می‌سازند. همه‌ی این امتیازات معمولا برای ایجاد اطمینان بین صاحب محتوای دیجیتالی و کاربر استفاده می‌شوند. در واقع مدیریت حقوق دیجیتال یک زنجیره‌ی ارزش برای محتواهای دیجیتال است، و به چرخه‌ی حیات محتوای دیجیتالی از ایجاد و بسته‌بندی تا انتشار اطلاعات برای استفاده و به اشتراک‌گذاری اشاره دارد. بنابراین، سیاست‌های امنیتی، اعتماد چندجانبه و مدیریت ریسک موجود در سیستم‌های عمومی مدیریت حقوق دیجیتال از اهداف مالکیت/تبادل محتوا و به اشتراک‌گذاری محتوا پشتیبانی می‌نماید[۸].

۳. مروری بر کارهای مرتبط

با وجود اینکه تئوری‌های پیشنهادی در پژوهش‌های انجام شده در غالب موارد مبتنی بر رمزنگاری می‌باشند، با این حال تکنیک‌های دیگری همانند نهان‌نگاری و رمزنگاری مبتنی بر هویت نیز در کنار آن مطرح شده است.

در ابتدا به مرور کارهایی می‌پردازیم که به طور انحصاری از تکنیک‌های رمزنگاری بهره برده‌اند. هرچند تئوری‌های رمزنگاری قوی و پیشرفته برای حل مشکل انتشار امن محتوای دیجیتال به گرفته می‌شود، ولی متاسفانه یک تئوری قابل قیاس برای مشکل مدیریت حقوق دیجیتال هنوز مطرح نشده است[۹]. فازیو در [۱۰] به طور سیستماتیک تحقیقی بر روی تکنیک‌های رمز برای بهبود رمزنگاری اولیه‌ی موجود در سیستم‌های مدیریت حقوق دیجیتال، با هدف گسترش کاربرد آنها در سناریوی مدیریت حقوق دیجیتال و تقویت فاکتورهای امنیتی انجام داده‌است. بر اساس تجزیه و تحلیل انجام شده در [۱۰]، در نهایت یک الگوی رمزنگاری کلید عمومی کارآمد برای گیرنده‌های بدون حالت به نمایش گذاشته شده است. اصطلاح گیرنده‌های بدون حالت برای دستگاه‌هایی همانند گیرنده‌های ماهواره که به طور ثابت برخط نمی‌باشند، به کار می‌رود.

محققان در [۱۱] از یک ایده‌ی جدید برای مدیریت حقوق دیجیتال بهره می‌گیرند. روش پیشنهادی آنها متشکل از رمزنگاری ناقص[۲] مبتنی بر ویژگی‌های کد هافمن با طول ثابت و مکانیزم شناسایی کاربر به منظور کنترل کیفیت مطالب دیجیتال است. به منظور پیاده سازی رمزنگاری

2 .Incomplete

ناقص طول کد هافمن با ضریب DCT در کدک جی‌پگ[3] اتخاذ می‌گردد. نویسندگان این مقاله در سال ۲۰۱۳ در پژوهش دیگر خود [۱۲] ترکیبی از کدهای دیفرانسیل و روش انگشت‌نگاری[4] مبتنی بر رمزنگاری ناقص را برای کارآیی و امنیت بهتر پیشنهاد داده‌اند. استفاده از روش‌های بیومتریک در این رویکرد علاوه بر منحصر بودن به فرمتی خاص یعنی جی‌پگ از دیگر محدودیت‌های این روش به شمار می‌رود.

جانگ و همکارانش [۱۳] یک سیستم رمزنگاری متقارن برای حفاظت از داده‌های چندرسانه‌ای با استفاده از ماتریس پازل ارائه داده‌اند. ویژگی اصلی این مقاله استفاده از الگوریتم تولید کلید به جای نگهداری کلید متقارن است. سیستم پیشنهادی از چند کلید خصوصی در واحد امنیتی سرور خود برای جلوگیری از دسترسی غیر قانونی کاربران استفاده می‌کند. از جمله محدودیت‌های سازوکار مطرحی توسط جانگ و همکارانش این است که بسیاری از رویکردهای مورد نظر مقاله تنها برای ویدئوها کاربرد دارند.

در حوزه‌ی نهان‌نگاری لیم و همکارانش در سال ۲۰۰۱ یک مدلی برای تایید تصاویر وب با استفاده از نهان‌نگاری نامحسوس ارائه دادند. در این مدل هرکاربر مجاز با یک دسترسی معتبر می‌تواند یک تصویر با استفاده از نهان‌نگاری تولید کند. فرانکو و همکارانش نیز یک پروتکل نهان‌نگاری در وب ارائه کرده‌اند. این مدل مبتنی بر چهار عامل کاربر، فروشنده، صدور گواهی نهان‌نگاری و سرور برای اطمینان از حفاظت در برابر کپی‌رایت اتخاذ شده است[۷]. در دیگر مدل‌های پیشنهادی مبتنی بر رمزنگاری در کنار بکارگیری تکنیک‌های رمزنگاری و نهان‌نگاری از روش‌های بیومتریک نیز استفاده شده است[۱۴]. هرچند استفاده از روش‌های بیومتریک امنیت را تا حد زیادی افزایش می‌دهد، با این حال محدودیت‌هایی را برای کاربران فراهم می‌کند.

رمزنگاری مبتنی بر هویت[5] نیز به عنوان روشی مناسب و پرکاربرد، در سیستم‌های مدیریت حقوق دیجیتال مطرح می‌باشد. این نوع رمزنگاری به یک نهاد مورد اعتماد نیازمند است، که مسئولیت ایجاد کلیدهای عمومی و خصوصی را بر عهده بگیرد. در همین رابطه دوتا و همکارانش[۱۵] الگویی برای مدیریت کلید در سیستم‌های مدیریت حقوق دیجیتال ارائه داده‌اند. این مدل علاوه بر کاربران نهایی و سرور اصلی شامل چندین توزیع‌کننده است که به کاربران خود اجازه می‌دهد، توزیع‌کننده‌ی دلخواه را براساس معیارهایی نظیر نزدیکی و یا تخفیف/ترقی قیمت انتخاب نمایند. در پژوهشی دیگر ایزومی و همکارانش[۱۶] به منظور حل مشکل مدیریت کلید در سیستم‌های مدیریت حقوق دیجیتال، با اضافه کردن اطلاعات بیومتریک به کلید، آن را به طور امن در داخل کارت هوشمند ذخیره می‌نمایند. در این روش نیز، آنها از رمزنگاری مبتنی بر هویت استفاده کرده‌اند. استفاده از این رمزنگاری مبتنی بر شناسه محدودیت‌هایی را نیز در حالت برون‌خطی ایجاد می‌نماید، و منحصر به حالت‌های برخط می‌باشد.

موضوع بعدی کنترل دسترسی الکترونیکی داده‌ها در سیستم‌های مدیریت حقوق دیجیتال متعارف و معمول است، که تنها به کاربران مجاز اجازه‌ی دسترسی به اسناد دیجیتال را می‌دهد. به همین منظور چن و همکاران در سال ۲۰۰۸، لین و همکاران در سال ۲۰۰۹ و چانگ و همکاران در سال ۲۰۱۰ نیز پیشنهاد سیستم مدیریت حقوق دیجیتال خود را مطرح کردند. چانگ و همکارانش [۱۷] نیز به ارائه‌ی مدلی در این رابطه پرداخته‌اند، که به اعتقاد خودشان بسیاری از مشکلات سیستم‌های پیشین در قسمت‌های انتقال غیرضروری و نشت داده‌ها و همچنین هزینه‌های بالا برای محاسبات را دارا نمی‌باشد. در روش پیشنهاد شده در این مقاله، از کارت‌های هوشمند برای کمک به تأیید درخواست کاربران و اجازه‌ی کاربران مجاز به دسترسی داده‌ها استفاده می‌شود. توجه به این نکته نیز قابل توجه است که عدم پشتیبانی از کنترل و نظارت بر فایل‌های داده‌ای در حالت برون‌خطی از مشکلات این رویکرد تلقی می‌گردد.

3.JPEG

4. Fragile Fingerprinting

5 .Identity-Based Encryption (IBE)

در پژوهشی دیگر با رویکرد اعتماد به کنترل اسناد دیجیتال می‌پردازند. یو و همکارانش مدلی مبتنی بر اعتماد[۶] طراحی کرده‌اند.[۱۸] در این مدل، محتوا همواره تحت کنترل مجوزها بوده و از حمله‌ی تکرارجلوگیری می‌شود. اعتماد متقابل میان اعضای یک سیستم مدیریت حقوق دیجیتال به منظور حمایت و حفاظت از محتوای الکترونیکی عاملی بسیار مهم و ضروری است.

۴. سیستم پیشنهادی

به طور کلی سیستم‌های مدیریت حقوق دیجیتال در دو حالت اصلی متصور هستند. در حالت اول محتوای دیجیتال در سمت کاربران نهایی به صورت رمزشده ذخیره می‌گردد، که این امر مستلزم وجود کلید رمزگشایی در هربار استفاده از داده‌های رمزشده است. نکته اینجاست که در این حالت کلید چگونه و در کجا بایستی محافظت گردد. در حالت دوم محتوای دیجیتال پس از نخستین رمزگشایی در قالب اصلی خود نگهداری می‌شود. در واقع در این حالت هیچ نظارت وکنترلی بر روی داده‌های دیجیتال پس از رمزگشایی وجود ندارد، و این مغایر با اهداف سیستم‌های مذکور است.

ایده‌ی اصلی روش پیشنهادی این است که کلید در حین اجرای الگوریتم به منظور رمزگشایی محتوای دیجیتال تولید می‌گردد، و این برخلاف اکثر سیستم‌های موجود است که مدیریت کلید در آنها با ذخیره‌ی کلید همراه است. همانطور که می‌دانید نگهداری از کلید در سمت کاربر از لحاظ فنی تبعاتی را به دنبال دارد. زیرا چنانچه کلید رمزگشایی در یک فایل معمولی ذخیره گردد، تبدیل محتوای دیجیتال به قالب اصلی به راحت‌ترین شکل ممکن صورت می‌گیرد. و در غیراینصورت اگر هکرها در بدست آوردن کلید توفیق نیابند، می‌توانند کلید محافظت شده را به همراه محتوای دیجیتال انتقال دهند.

محافظت از الگوریتم تولید کلید رمزگشایی نیز بسیار حائز اهمیت می‌باشد. به عبارت دیگر اگرچه استفاده از این الگوریتم و جایگزینی آن با ذخیره‌ی کلید تا حد زیادی کلید را از دسترس کاربران غیرمجاز دور نگه می‌دارد، ولی درصورتیکه این افراد به الگوریتم دست یابند و از محتوای آن آگاهی یابند، تولید کلید کار آسانی است. برای حل مشکل مذکور نیز ما نیازمند این هستیم که به نوعی کلید را به اطلاعات متمایز کاربر وابسته نماییم. به طور معمول هر رایانه‌ای دارای اطلاعات متمایز و یکتاست. که از جمله‌ی آنها می‌توان به شناسه‌ی CPU و شناسه‌ی Hard Drive اشاره نمود. با درنظرگرفتن این اطلاعات، بدست آوردن الگوریتم و ساختن کلید رمزگشایی برای کاربران غیر مجاز کارایی نخواهد داشت.

۱.۴ تولید کلید رمز سمت سرور

در قدم اول برای تولید کلید، داده‌های زیر را دریافت می‌نماییم:

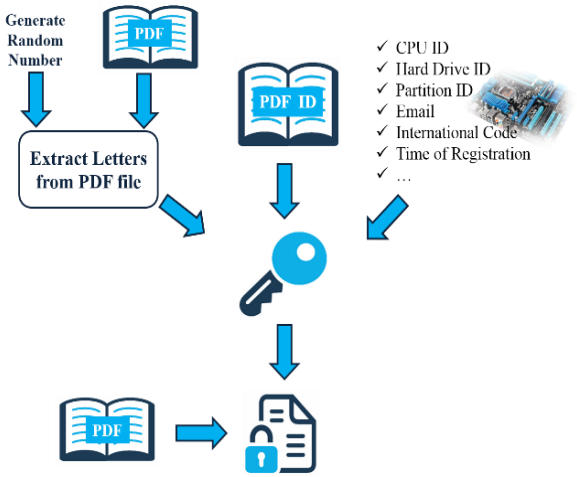
۱. داده‌های یکتا و متمایز
   - شناسه‌ی CPU
   - شناسه‌ی Hard Drive
   - زمان ثبت نام
   - کدملی
   - ایمیل
۲. داده‌های وابسته به محتوای دیجیتال
۳. شناسه‌ی یکتای محتوای دیجیتال

شمای کلی تولید کلید رمزگشایی با استفاده از اطلاعات بالا در شکل ۱.۴ نشان داده شده است. گفتنی است محتوای دیجیتال مورد نظر در این پژوهش، قالب پی‌دی‌اف می‌باشد.

داده‌های یکتا همانند شناسه‌ی CPU، کدملی، ایمیل کاربر و غیره در هنگام ثبت‌نام کاربران دریافت می‌شوند، و سایر داده‌ها نیز توسط خود مؤلف تولید و ذخیره می‌گردند. اینکه کدامیک از داده‌های یکتا موثر در ساخت کلید باشند موضوعی است که به طور تصادفی مشخص می‌شود. از سوی دیگر مؤلف نیز که دارای مجموعه‌ای وسیع از فایل‌ها و به طور خاص کتاب‌ها می‌باشد، برای هریک از آنها یک شناسه‌ی منحصر به فرد ایجاد می‌نماید.

دسته‌ی دیگری از داده‌ها وابسته به محتوا هستند که براساس الگوریتم طراحی شده، بدست می‌آیند. برای بدست آوردن حروف تصادفی از صفحه‌ی اول به این ترتیب عمل

6 .Trusted Platform Module(TPM)



شکل ۱.۴ – تولید فایل رمزشده در سمت سرور

می‌کنیم، که در ابتدا با استفاده از توابع رندم[۷] ۳ عدد تصادفی را تولید می‌نماییم. این سه عدد را i، j و k و در بازه ی [1-22] در نظر بگیرید. در صفحه‌ی مقدمه‌ی کتاب به خط iام رفته و حرف jام را استخراج می‌کنیم. سپس به خط jام رفته و حرف kام را انتخاب می‌کنیم. پس از آن به خط kام رفته و حرف iام را بر می‌داریم. در انتها به سه حرف از صفحه‌ی مقدمه دست پیدا می‌کنیم، که تشکیل دهنده‌ی بخشی از کلید می‌باشند.

در نهایت کلید رمز با بکارگیری تابع هش و از رابطه‌ی ۱ بدست آمده، و در قدم بعدی محتوای دیجیتال مورد نظر توسط آن رمز می‌گردد.

K_1 = داده‌های متمایز

K_2 = داده‌های وابسته به محتوا

K_3 = شناسه‌ی یکتای محتوا (۱)

$KEY=Hash(K_1 \| K_2 \| K_3)$

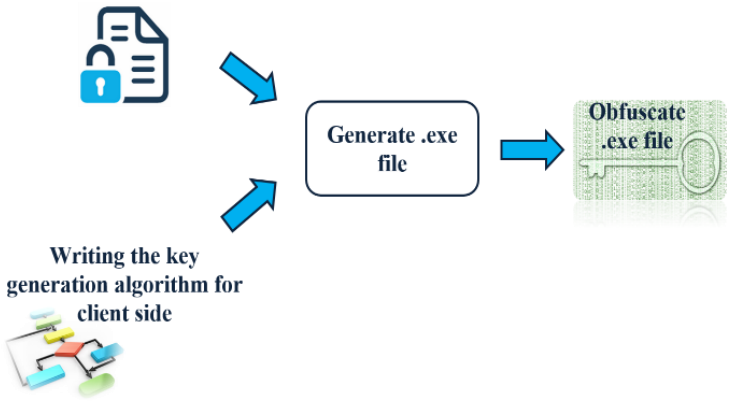
۲.۴ تولید الگوریتم اجرایی

پس از تولید کتاب رمز شده در مرحله‌ی قبل، باید به سراغ الگوریتمی برویم که بایستی توسط کاربر نهایی پس از دریافت فایل به منظور تولید کلید اجرا گردد. این الگوریتم شبیه الگوریتم ایجاد کلید در سمت سرور است، با این تفاوت که اطلاعاتی همانند شناسه‌ی CPU به طور مستقیم و با استفاده از کتابخانه‌ای، از سخت افزار کامپیوتر شخصی کاربر استخراج می‌گردد. این بدین معنی است که اطلاعات به هیچ وجه نمی‌توانند تقلبی باشند. به عبارت دیگر در کنار ارسال فایل دیجیتال به کاربر به الگوریتمی برای ساخت کلید در سمت کاربر نیاز داریم، و چنانچه فایل پی‌دی‌اف رمز شده به تنهایی به دست کاربر برسد، بدون وجود کلید امکان مشاهده و مطالعه‌ی آن وجود نخواهد داشت.

در نتیجه داده‌های دیجیتال به همراه الگوریتم اجرایی برای تولید کلید در قالب یک فایلexe. و پس از انجام عملیات مبهم‌سازی برای کاربر فرستاده می‌شوند، و کاربر به جای دریافت فایل رمزشده و کلید به طور جداگانه، یک فایل اجرایی را بدست می‌آورد.

به عبارت دیگر مبهم‌سازی در آخرین مرحله‌ی تولید فایل ارسالی به کاربر، با افزایش پیچیدگی در الگوریتم، کار کاربران غیرمجاز را برای بدست آوردن اطلاعات تا حد قابل قبولی سخت می‌نماید. جابجایی کد، جایگزینی کد با کد مشابه و افزایش دستورالعمل در داخل کد به عنوان روش‌های مبهم‌سازی، از مهندسی معکوس جلوگیری می‌نماید. در شکل ۲.۴ مراحل تولید فایل اجرایی را مشاهده می‌نمایید.

7 .Random



شکل ۲.۴ – مراحل نهایی تولید فایل ارسالی برای کاربر

جدول ۱.۵ – مقایسه‌ی بین سیستم‌های موجود و روش پیشنهادی

پارامتر	DRM-X3	Editionguard	Fidibo	سیستم پیشنهادی
روش رمزنگاری	رمزنگاری نامتقارن	رمزنگاری متقارن	رمزنگاری متقارن	رمزنگاری متقارن
پشتیبانی در حالت برون‌خطی	اتصال به اینترنت برای مدیریت کلید مورد نیاز است	اتصال دائم به اینترنت مورد نیاز است	نیازی به اتصال دائم به اینترنت نیست	نیازی به اتصال دائم به اینترنت نیست
کپی‌برداری	عدم امکان	امکان	امکان	عدم امکان
وابستگی به محتوای دیجیتال	کلید به صفحات محتوا وابسته نیست	کلید به صفحات محتوا وابسته است	کلید به صفحات محتوا وابسته نیست	کلید به صفحات محتوا وابسته است
نیازمند به برنامه‌ی کاربردی خاص	وابسته به نرم‌افزار Haihaisoft PDF Reader	وابسته به نرم‌افزار Adobe Digital Edition	وابسته به نرم‌افزار فیدیبو	عدم وابستگی به نرم‌افزار خاص
مبهم‌سازی	عدم بکارگیری	عدم بکارگیری	عدم بکارگیری	بکارگیری

در پایان کلید رمزگشایی پس از اجرای محتوای نهایی توسط کاربر، با استخراج حروف از متن و دریافت شناسه‌های یکتا، تولید می‌گردد. در نتیجه کاربر نهایی با در دست داشتن این کلید، قادر به رمزگشایی فایل دیجیتال و در نهایت استفاده از آن خواهد بود. گفتنی است اگرچه روند تولید کلید در هر بار استفاده از محتوای دیجیتال یکسان است، با این حال کلید در جایی ذخیره نمی‌گردد و امکان دسترسی مستقیم به آن با دشواری‌هایی همراه است.

۵. ارزیابی سیستم پیشنهادی

کارایی روش پیشنهادی برای سیستم‌های مدیریت حقوق دیجیتال را با معیارهای مختلفی می‌توان سنجید. بدین منظور سه نرم‌افزار کتابخوان فیدیبو، Editionguard و DRM-X3 را برای مقایسه درنظر می‌گیریم. سیستم پیشنهادی از لحاظ معیارهای روش رمزنگاری، پشتیبانی در حالت برون‌خطی، عدم امکان کپی‌برداری، وابستگی کلید به محتوای دیجیتال، نیازمندی به برنامه‌ی کاربردی خاص و

مبهم‌سازی در برابر سیستم‌های فوق ارزیابی می‌گردد. نتایج این مقایسه در جدول ۱.۵ قابل مشاهده می‌باشد. اطلاعات در دسترس برای ارزیابی در مورد برخی از معیارها براساس کار با نرم‌افزارها و در مورد برخی دیگر در نتیجه‌ی اطلاعات موجود و همچنین ارتباط با کارشناسان مربوطه جمع‌آوری شده است.

در بیشتر سیستم‌های امنیت اطلاعات از کلید متقارن برای رمزنگاری استفاده می‌نمایند. این روش بستگی به مخفی‌بودن کلید دارد، و بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا در جایی که کلید بین دو سیستم که قبلا هویت یکدیگر را تایید کرده‌اند، مبادله گردد. از مزایای عمده‌ی رمزنگاری متقارن می‌توان به رمزنگاری و رمزگشایی سریع و بازده بالای آن اشاره نمود. ما نیز در این پژوهش از کلید متقارن بهره می‌گیریم.

دغدغه‌ی اصلی سیستم‌های مدیریت حقوق دیجیتال با ارسال فایل‌های دیجیتال به کاربران نهایی آغاز می‌گردد، و در نتیجه بایستی مکانیزمی اتخاذ گردد که در صورت قطع ارتباط با اینترنت مؤلفان و صاحبان حقوق از عدم کپی‌برداری محتوای خود اطمینان حاصل نمایند. از امتیازات روش پیشنهادی پشتیبانی از محتوای دیجیتال در حالت برون‌خطی[8] است. برخلاف رویکرد مقالات [۱۴،۱۳،۱۲،۳] که وابسته به حالت برخط هستند، ایده‌ی این روش مبتنی بر کنترل و نظارت از داده‌های دیجیتال در جمیع حالات می‌باشد.

از طرف دیگر مدیریت کلید در سیستم‌های مدیریت حقوق دیجیتال باید به گونه‌ای باشد که فروشنده‌ی کتاب، ناشر و مؤلف مطمئن باشند که خریدار، یک نسخه‌ی دیجیتالی غیرمجاز از این کتاب دیجیتالی ایجاد نمی‌نماید، و با استفاده از کپی‌برداری محتوای آن را در همه جا توزیع نمی‌کند. این در حالی است که در برخی از نرم‌افزارها در صورت کپی‌برداری با داشتن نام کاربری و رمزعبور کاربر مجاز، امکان مشاهده‌ی محتوای الکتریکی در سیستم دیگر وجود خواهد داشت. از اینرو برای رسیدن به این مهم، استفاده از داده‌های یکتا و متمایز همانند شناسه‌ی CPU یا Hard Drive به عنوان بخشی از داده‌های کلید متقارن امری ضروری تلقی می‌گردد. چراکه با فرض انتقال داده‌ها از آنجاکه این شناسه‌ها برای هر رایانه متمایز هستند، در هر صورت امکان استفاده از محتوای دیجیتال وجود نخواهد داشت.

همانطور که در بخش ۴ هم بدان اشاره شد، داده‌های وابسته به محتوا به عنوان جزئی دیگر از اطلاعات کلید محسوب می‌شوند. با توجه به اینکه مدیریت کلید شامل تولید، ارسال و نگهداری کلیدها می‌باشد، بکارگیری داده‌های وابسته به محتوا به طور خاص برای نگهداری امن کلید بسیار حائز اهمیت است. حالتی را فرض کنید که کاربر غیرمجاز به الگوریتم تولید کلید دست یافته است. در اینصورت چنانچه بخواهد از کلید موردنظر به سایر محتواهای دیجیتال آن مؤلف خاص دست یابد، توفیقی کسب نمی‌کند. از آنجایی که این دسته از داده‌ها براساس اعدادی تصادفی استخراج می‌گردد، در صورت یافتن مراحل الگوریتم باز هم موفق به ساخت کلید برای همه‌ی فایل‌ها نمی‌گردد.

از دیگر مزایای سیستم پیشنهادی عدم وابستگی آن به برنامه‌ی کاربردی خاص است. همانطور که در جدول ۱.۵ نیز مشاهده می‌نمایید، هرکدام ازسیستم‌های درنظرگرفته شده به منظور استفاده در سمت کاربر نیازمند نرم‌افزاری خاص می‌باشند. در حالیکه در رویکرد ارائه شده به منظور راحتی کاربران تنها از نرم‌افزار Adobe Reader بهره‌گیری می‌شود، که نرم‌افزاری معمول برای مشاهده‌ی فایل‌هایی با فرمت پی‌دی‌اف است.

آخرین معیاری که به ما برای ارزیابی عملکرد سیستم پیشنهادی کمک می‌نماید، استفاده از تکنیک‌های مبهم‌سازی است. امروزه مهندسی معکوس، سرقت نرم‌افزار و دستکاری نرم‌افزار از جمله تهدیدهای رایج در برابر نرم‌افزارهای با مالکیت خصوصی می‌باشند. استخراج الگوریتم‌های اختصاصی و استفاده از آنها در برنامه‌های شخصی، غیرقانونی است. با این حال، با مهندسی معکوس الگوریتم‌ها و درک رفتار درونی آنها، زمان و هزینه‌ی توسعه‌ی الگوریتم‌های مشابه کاهش یافته، و در نتیجه

8. Offline

مبهم‌سازی می‌تواند از الگوریتم‌های پرارزش محافظت نماید. در همین راستا با توجه به عدم ذخیره‌ی کلید رمزگشایی در رویکرد ارائه شده، محافظت از الگوریتم تولید کلید بسیار حائز اهمیت می‌باشد. چراکه هکرها در صورت بدست آوردن اطلاعات داخل الگوریتم، به راحتی می‌توانند کلید را استخراج نمایند و این چالشی بزرگ برای ناشران تلقی می‌گردد.

۶. جمع‌بندی و نتیجه‌گیری

مدیریت حقوق دیجیتال یک فناوری مدیریتی است که موجب حفاظت، توزیع و بهره‌گیری از حقوق مالکیت معنوی در مورد اسناد دیجیتال در محیط‌های امن می‌گردد. سیستم‌های موردنظر از دسترسی غیرمجاز کاربران جلوگیری نموده و در نهایت از حقوق و منافع یک نویسنده حمایت می‌نمایند. با این حال سیستم‌های موجود به منظور جلوگیری از افشای کلید رمزنگاری، با محدودیت‌های بسیاری در رابطه با روش رمزنگاری، پشتیبانی در حالت برون خطی و عدم امکان کپی‌برداری به عنوان مهم‌ترین معیارها مواجه می‌باشند. بر همین اساس در این مقاله مدلی مبتنی بر رمزنگاری برای مدیریت کلید در سیستم‌های مدیریت حقوق دیجیتال ارائه گردید. در این مدل، کلید با استفاده از سه دسته اطلاعات وابسته به محتوا، اطلاعات یکتا و شناسه‌ی یکتای محتوای دیجیتال بدست می‌آید. وجود داده‌های متمایز در کلید موجب می‌گردد تا کاربران غیر مجاز امکان استفاده از داده‌ها را در محیطی غیرقانونی نداشته باشند. همچنین وابستگی کلید به محتوای دیجیتال، جهت نگهداری امن کلید بسیار مؤثر خواهد بود. به طور کلی مدل ارائه شده در این پژوهش به دنبال آن است که دستیابی هکرها به کلید و الگوریتم اجرایی را تا حد ممکن سخت نماید. استفاده از شناسه‌ی یکتای محتوای دیجیتال هم دلیلی بر این ادعا می‌باشد. از دیگر نقاط قوت الگوریتم پیشنهادی این است که نسبت به سیستم‌های مشابه قابلیت پشتیبانی از فایل‌های دیجیتال در حالت برون‌خطی را نیز دارا می‌باشد. از اینرو جهت جلوگیری از کپی‌برداری نیازی به اتصال دائم به اینترنت نمی‌باشد. در مقالات آینده تکنیک‌های مبهم‌سازی و نحوه‌ی محافظت از کلیدها و پیچیدگی محاسباتی بدست آمده از تکنیک‌های به کارگرفته شده در این پژوهش، ارائه خواهد شد.

مراجع

1. A.C.Prihandoko, B.Litow, H.Ghodosi, "DRM's rights protection capability: a review", International Conference on Computational Science and Information Management, 2012.

2. J.He, H.Zhang, "Digital Right Management Model Based on Cryptography and Digital Watermarking", International Conference on Computer Science and Software Engineering, 2008.

3. C. L.Pimentel. R.Monroy, V.F.R.Fon Bon, "Symmetric Cryptography Protocol for Signing and Authenticating Digital Documents", Springer-Verlag, *Berlin Heidelberg*, pp. 9–23, 2011.

4. L.Zheng, L.Feng, Y.Li, X.Cheng, "Research on Digital Rights Management Model for Spatial Data Files", 2nd International Conference on Information Engineering and Computer Science (ICIECS), Vol. 4, 2010.

5. A.M.Eskicioglu, "Key Management for Multimedia Access and Distribution" from "Multimedia Security Technologies for Digital Rights Management", ISBN: 9780-0-12-369476, Elsevier science, 2006.

6. Emilija Arsenova, MI, RWTH-Aachen, "Technical aspects of Digital Rights Management", Seminar: Digital Rights Management.

7. Mir Mohamad Azad, "Digital Rights Management", *IJCSNS International journal of Computer Science and Network Security*, November 2010.

8. Z.Zhang, "Digital Rights Management Ecosystem and its Usage Controls: A Survey", International Journal of Digital Content Technology and its Applications, Volume 5, Number 3, March 2011.

9.M.Stamp, DIGITAL RIGHTS MANAGEMENT: THE TECHNOLOGY

BEHIND THE HYPE, Journal of Electronic Commerce Research, VOL. 4, NO. 3, 2003.
10.N. Fazio, "On Cryptographic Techniques for Digital Rights Management", New York University, Sep. 2006.
11. M.Iwakiri, T.M.Thanh, "Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management", 26th IEEE International Conference on Advanced Information Networking and Applications, pp. 763-770, 2012.
12. T.M.Thanh, M.Iwakiri, "An Incomplete Cryptography based Digital Rights Management with DCFF", The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, March 2013.
13. Y.Jung, J.Kim, M.Jun, "DRM Encryption System using the Key Exchange with Matrix Puzzle", International Conference on Hybrid Information Technology, *IEEE Computer Society*, 2006.
14. C. L.Pimentel. R.Monroy, V.F.R.Fon Bon, "Symmetric Cryptography Protocol for Signing and Authenticating Digital Documents", Springer-Verlag, *Berlin Heidelberg*, pp. 9–23, 2011.
15. R.Dutta, S.Mukhopadhyay, T.Dowling, "Key Management in Multi-Distributor based DRM System with Mobile Clients using IBE", Applications of Digital Information and Web Technologies, Second International Conference on the, pp. 597 – 602, 2009.
16. A.Izumi, Y.Ueshige, K.Sakurai, "A proposal of efficient scheme of key management using ID-based encryption and Biometrics", International Conference on Multimedia and Ubiquitous Engineering, 2007.
17. E.Chang, K.H.Huang, A.B.Lu, F.Lai, "Enterprise Digital Rights Management System based on Smart Card", IEEE 15th International Symposium on Consumer Electronics, pp. 363-368, 2011.
18. A.Yu, D.Feng, R.Liu, "TBDRM: A TPM-Based Secure DRM Architecture", 2009 International Conference on Computational Science and Engineering.