حفاظت اطلاعات در آموزش الکترونیک
معرفی سیستم CIPRESS

سعید صافی، محمد رئوف ابراهیمی

چکیده

با توجه به آنچه در قسمت اول این مقاله آمد حفاظت از اقلام آموزشی طبق قوانین حق نشر، آموزش و امتحان در شرایط ایمن دارای اهمیت است. در این مقاله سیستم تقویت حقوق مالکیت معنوی بکمک رمزنگاری کامپیوتری (CIPRESS) معرفی گردیده است و اجزاء سیستم و روش کار آن بیان شده است. سپس توان بالقوه این سیستم و کاربرد ویژه‌ای که این سیستم می‌تواند در آموزش الکترونیک داشته باشد مورد بررسی قرار گرفته و مزایای آن نسبت به نرم‌افزارهای مشابه بیان شده است.

۱- حفاظت از مالکیت معنوی[1]

همانگونه که قبلا هم ذکر شد، مشکل اصلی در محافظت از داده‌های دیجیتال در شبکه جهانی (www) این است که عامل نظارت بر حق نشر[2] از زمانی که اقلام نشر یافته به صورت داده‌های دیجیتال به کاربر تحویل داده شدند کنترلش را بر آنها از دست می‌دهد و کاربر بدون اینکه خدشه‌ای بر کیفیت آن وارد شود می‌تواند، هر تعداد کپی که بخواهد تهیه نماید. یک شیوه برای کنترل مالکیت معنوی این است، که ناظر حق نشر بتواند، کنترل خود را بر تمام طول عمر داده‌های دیجیتال بسط دهد.

سیستم CIPRESS[3]، سیستم تقویت حقوق مالکیت معنوی به کمک رمزنگاری است که توسط شرکتهای Mitsubishi ژاپن وانستتیوی Fraunhofer آلمان برای توسعه مشترک در زمینه رمزنگاری کامپیوتری و برای حفاظت از مالکیت معنوی در مقابل استفاده‌های غیر مجاز ابداع شده است. این سیستم تسریع در استفاده‌های مجدد از اقلام دارای حقوق نشر، را با استفاده

1 - Intellectual Property

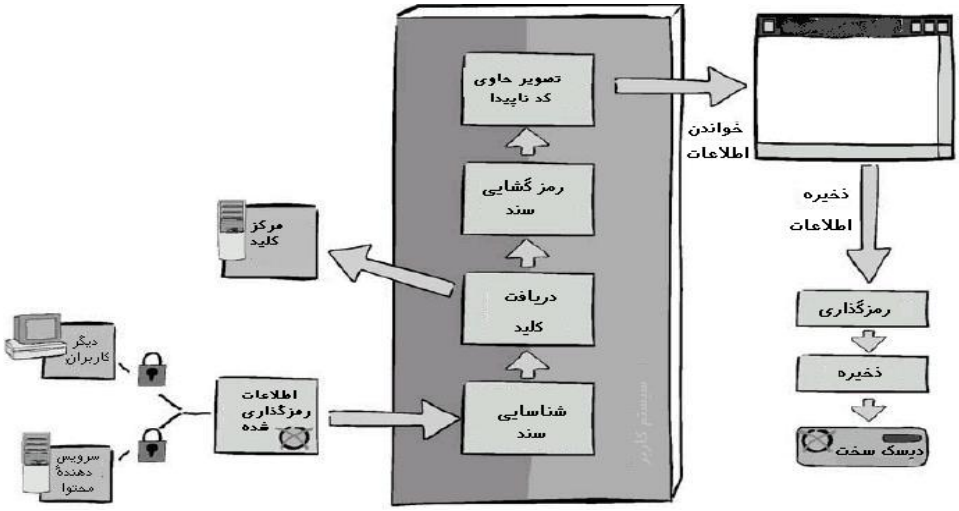
2 - Copyringht Holder

3 - Cryptographic Intellectual PropertyRights Enforcement System

از ترکیب دو سیستم ثبت شده رمزگذاری مجدد و تکنولوژی کدهای مخفی[1] محقق کرده است]۱[و (شکل ۱). بخش آتی ابتدا دور نمائی از این سیستم ترسیم می‌کند و سپس در مورد چگونگی استفاده از CIPRESS بحث خواهد شد.

۲- دور نمای CIPRESS

تکنولوژی رمزگذاری مجدد یک تکنولوژی کلیدی برای جلوگیری از توزیع غیر مجاز و همچنین تحت نظر داشتن دقیق استفاده از اسناد است. ایده اصلی در این زمینه این است که تمامی داده‌ها به شکل رمزگذاری شده بر روی ابزار ذخیره سازی کامپیوتر کاربر ذخیره شود (در CIPRESS عنوان کاربر یا client را به کامپیوتری اطلاق می‌کنند که به منظور دسترسی، نمایش و تغییر در اسناد مورد استفاده قرار می‌گیرد). نا گزیر اسنادی که قصد دسترسی به آنها وجود دارد، بایستی رمزگشائی شود ولیکن این رمزگشائی موقتی است، بنابر این اطلاعات و داده‌های رمزگشائی شده فقط در حافظهٔ موقت کامپیوتر وجود دارد و به محض اینکه سند بر روی ابزار ذخیره سازی منتقل شود دوباره رمزگذاری می‌شود.



شکل۱ - سیستم CIPRESS

نکته بغرنج این است، که CIPRESS کلید رمزگذاری قبلی را مجدداً استفاده نمی‌کند، بلکه یک کلید منحصر بفرد ایجاد می‌کند که مخصوص سند است. هر زمانی که سند نوشته شود، ایجاد کلید توسط مخزن مرکزی کلید انجام می‌شود که به اصطلاح مرکز کلید خوانده می‌شود. در CIPRESS کلیدها انحصاراً در مرکز کلید تولید می‌شوند بنابراین هر دسترسی به اسناد درون مرکز کلید به شکل یک کلید مربوط به آن دسترسی، وجود دارد. از این رو می‌توان از هر گونه استفاده از اسناد آگاهی یافت و آن را تحت نظر داشت. بعلاوه اگر مرکز کلید هیچ کلیدی برای یک سند ارائه نکند کاربر امکان دسترسی به آن را نخواهد داشت. در عمل این بدین معناست که یک مهاجم خارجی به اطلاعات این سیستم ممکن است داده‌ها یا تمام ابزار ذخیره‌سازی و حتی کامپیوتر را بدزدد ولی آنچه بدست می‌آورد، یک سری اطلاعات به شکل رمزگذاری شده است و به منظور مشاهدهٔ محتوای اسناد او بایستی با مرکز کلید تماس بگیرد و هویت خودش را اعلام کند تا کلید مورد نظر را بدست آورد. اگر او از شناسهٔ کاربری خودش استفاده کند مرکز کلید آن تماس را به عنوان یک تماس غیر مجاز تشخیص می‌دهد و کلیدی تحویل نمی‌دهد. بنابر این دزدیدن صرف داده‌ها و اطلاعات کافی نیست و مهاجم باید اعتبار یکی از کاربرانی که حق دسترسی کافی به اسناد را دارد را نیز داشته باشد. ازطرفی بانک کلید گزارشی از همهٔ دسترسی‌ها نگه می‌دارد بنابر این غیر ممکن است بدون اینکه هیچ ردی باقی بماند به داده‌ها دسترسی یافت. این واقعیت که با بررسی گزارشات بانک کلید رد پاهای استفاده از

1 - Water Marking

یک سند قابل بازیابی است، یک شاخصهٔ اساسی امنیتی است زیرا زمانی که ناظر حق نشر یکی از نسخه‌های دزدیده شده از اسنادش را می‌یابد. این مشخصه در اثبات مالکیتش بر آن نسخه و همچنین تشخیص حفرهٔ امنیتی سیستم کمک می‌کند.

تمام این فرایندها رمزگذاری و رمزگشائی به طور شفافی توسط یکی از اجزا سیستم CIPRESS انجام می‌شود. این اجزاء CIPRESS، HASH رمزنگاری سند را به منظور بازیابی کلید مربوط به آن سند از مرکز کلید مورد استفاده قرار می‌دهد. یک عصاره[1] سند را می‌توان به عنوان یک شناساگر منحصر بفرد برای هر سند در نظر گرفت. به روشی محاسبات انجام می‌شود که با احتمال مناسبی این اطمینان حاصل شود که برای دو متن متفاوت که حتی می‌توانند در یک بیت تفاوت داشته باشند هرگز دو عصاره مشابه محاسبه نشود. این بدین معناست که اگر زمانی، کاربری محتویات یک سند را تغییر دهد با سند تغییر یافته در CIPRESS بعنوان یک سند جدید رفتار می‌شود. اجباری که در ثبت تمامی فایلهای سیستم و درخواستها و ثبت آنها هر زمانی که فایلی تغییر کند وجود دارد ترافیک شبکه و سرریز عظیمی از اطلاعات در مرکز کلید را باعث خواهد شد، بخصوص که در هنگام ورود کاربران[2] سیستم بسیاری از فایل‌های سیستم تغییر خواهد کرد. به همین علت است که CIPRESS برای استفاده‌های غیر مشترک از اسناد محلی بر روی ابزار ذخیره سازی سرویس گیرنده‌ها و کاربران پشتیبانی می‌کند و درست مثل اسناد خود CIPRESS این اسناد نیز به صورت اتوماتیک رمزگذاری و رمزگشایی می‌شوند ولی بجای استفاده از فرایند رمزگذاری مجدد و گرفتن کلید از مرکز کلید یک کلید مختص به هر ماشین که کلید اصلی[3] گفته می‌شود مورد استفاده قرار می‌گیرد. این کلید اصلی رمزگذاری برای هر سرویس گیرنده CIPRESS مختص به خود است بنابراین متنی که توسط یک کلید اصلی رمزگذاری شده است فقط بر روی کامپیوتری که آن را رمزگذاری کرده است قابل دسترسی است. وقتی که فرآیند رمزگشایی یک سند تکمیل شد و امکان دسترسی عمومی به آن فراهم شد بایستی این سند توسط CIPRESS ثبت شود. از آن پس بر روی سند رمزگذاری با استفاده از کلیدهای مرکز کلید انجام می‌شود و بنابراین تحت کنترل بر استفاده مرکز کلید و نظارت دائم آن قرار می‌گیرد. انجام عملیات ثبت باید بر روی سرویس دهنده محتوا[4] انجام شود در CIPRESS سرویس دهنده محتوا بمنظور ذخیره مجتمع و دائم اسناد دیجیتال استفاده می‌شود. اسناد می‌توانند به هر یک از اشکال چند رسانه‌ای مانند داده‌های متنی، صوتی، تصویری و تصاویر باشند. کاربر می‌تواند اسناد را از سرور محتوا یا با استفاده از درخواستهای مخصوص CIPRESS که خود مستلزم ثبت آن سند است یا با استفاده از شبکه جهانی اینترنت بوسیله هر مرورگر صفحه‌های وب که بر روی یکی از سرویس گیرندگان CIPRESS قرار دارد بدست آورد. بر روی سرویس دهندگان استاندارد فایل نیز می‌توان به اقلام رمزگذاری شده دسترسی یافت.

از دیدگاه فنی سیستم CIPRESS از لایه الحاقی کمتری، نیست به سیستم عامل برخوردار است. چنین الحاقاتی به سیستم عاملها برای ویندوز NT4.0، 2000، Solaris گسترش داده شده‌اند. بنابراین CIPRESS یک لایه مستقل از تقاضا فراهم می‌کند. شاخصه‌های امنیتی CIPRESS به طور شفافی به سیستم اضافه شده است بدون اینکه هیچ تقلیدی از نرم افزارهای بازاری در خود داشته باشند. از دیگر جنبه‌های CIPRESS با این مشخصه آن تحقق می‌یابد که می‌تواند بعنوان یک الحاق بر سیستم عامل سرویس گیرندگان عمل نماید و یمنظور تضمین کارکرد صحیح این الحاق، کاربر عادی نمی‌بایست قادر به بهم ریختن و سوء استفاده از اجزای سیستم، با آشنایی از الحاقات آن باشد. بنابراین استفاده از CIPRESS محدود به سیستم عاملهای می‌شود که چنین حفاظتی ایجاد کنند و بتوانند محیط‌هایی فراهم آورند که مدیریت کامپیوتر سرویس گیرنده در دست افراد قابل اطمینان قرار گیرد. CIPRESS مدیریت کاربران خودش و گروهها را انجام می‌دهد، این مدیریت همچنین پایه‌ای برای حقوق ویژه دسترسی CIPRESS است. بنابراین CIPRESS می‌توانند به صورت عمومی مورد استفاده قرار گیرد بدون اینکه با مکانیزم‌های حفاظتی که توسط برخی سیستم عاملها اعمال می‌شود محدود شود.

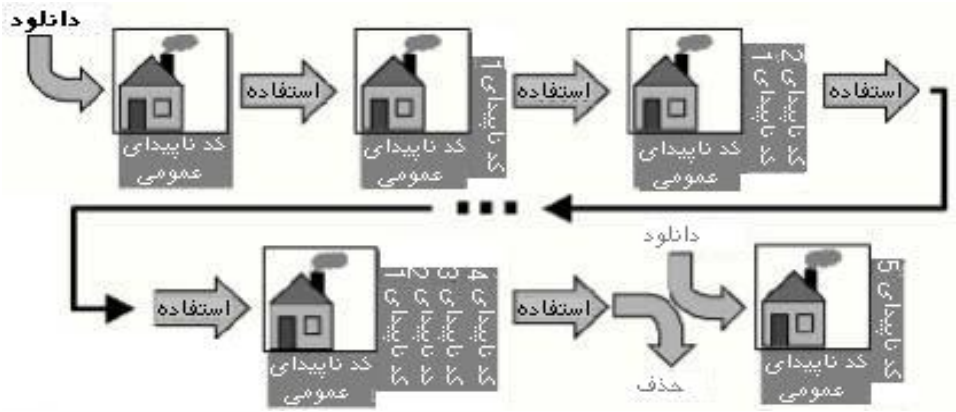
1- Digest
2 - Log In
3 - Master Key
4 - Content Server

تا کنون بحث ما به دسترسی به اسناد از ابزار ذخیره سازی اختصاص داشت. ولی به منظور ارتباط و مشارکت با دیگر کاربران این سیستم باید قابلیت توزیع اسناد از طریق شبکه را نیز داشته باشد بنابراین یکی از اجزای CIPRESS تمامی ترافیک ورودی و خروجی را تحت نظر دارد. این مؤلفه وقتی داده‌های رمزگذاری شده CIPRESS را دریافت می‌کند به سرعت داده‌ها را رمزگشایی می‌کند. در مواردی که ارتباط با یک کامپیوتر خارج محدودهٔ امنیتی بر قرار می‌شود این مولفه از SSL برای کدگذاری ارتباط استفاده می‌کند بنابراین مانند شبکه‌های خصوصی مجازی[1] این مولفه CIPRESS تضمین می‌کند که اطلاعاتی که از طریق محیط اینترنت نا امن منتقل می‌شود در بین راه مورد سوء استفاده و استراق سمع قرار نگیرد. برای تضمین قابلیت اطمینان، CIPRESS فقط ارتباط ssl را بین میزبانهای مطمئن بر قرار می‌سازد و همچنین ارتباط بین دو کامپیوتر CIPRESS در درون یک محیط امنیتی مشابه نبایستی کد گذاری شود.

ترکیبی از این دو مکانیزم به تمام کانالهای ارتباطی توزیع اطلاعات، که یک کامپیوتر با آن درگیراست امنیت کافی می‌بخشد. با این وجود در بعضی روشهای سرقت اطلاعات نمی‌توان از تمامی مؤلفه‌های سیستم امنیتی چنین کامپیوترهایی بهره برداری کامل کرد مثلاً از زمانی که از صفحه نمایش کپی، عکس یا فیلم گرفته می‌شود هیچ سیستم نرم افزاری قادر به ممانعت از چنین حمله‌هایی نیست و ممانعت از این کار باید با ابزارهای اجرایی انجام شود. ولی CIPRESS می‌تواند موجب شود تا چنین حمله‌هایی برای مهاجمان که اغلب از درون دستگاهها هستند کارهای خطرناک تری به حساب آیند بر اساس بر آورده‌های FBI شانس موفقیت در تحت پیگیرد قرار دادن چنین افرادی یک در ۲۲۰۰۰ مورد است[۱]. همانگونه که قبلا نیز بیان شد CIPRESS از کلید خصوصی برای رمزگذاری استفاده می‌کند که ردیابی استفاده کننده‌هایی که امکان دسترسی به یک نسخه خاص از یک سند را دارند فراهم می‌کند. این اطلاعات در مورد استفاده افراد از سندها، فقط در درون کلیدهای کد گذاری قرار دارد که با خروج داده‌ها از کامپیوتر از دست می‌روند در عوض CIPRESS این اطلاعات را در درون اطلاعات اسناد به صورت کدهای ناپیدای دیجیتال مخفی می‌کند. تکنولوژی کدهای ناپیدا در مورد تصاویر و فایلهای تصویری در CIPRESS از این لحاظ منحصر فرد است که CIPRESS کدهای ناپیدایی با قابلیت سلسله مراتبی فراهم می‌کند [۳و۲]. به این ترتیب که هر کد ناپیدا موجب اندکی کاهش در کیفیت تصاویرمی‌شود و این کاهشها کم‌کم با هم تجمع می‌یابند. CIPRESS حداکثر به پنج بار اعمال کدهای ناپیدا اجازه می‌دهد (شکل ۲). اولین کد، کد ناپیدای عمومی است، این کد ناپیدا به محض ثبت شدن سند درون آن قرار می‌گیرد و شناسهٔ نگهدارنده حق نشر را در خود دارد. با خوانده شدن این کدهای ناپیدای عمومی می‌توان نگه دارنده حق نشر مربوط به آن سند بخصوص را تشخیص داد. این مسئله از اهمیت بالایی برخوردار است زیرا نگه دارنده حق نشر می‌تواند ادعای مالکیتش بر آن سند را به راحتی در دادگاه ثابت کند. چهار کد ناپیدای دیگر محرمانه هستند. هر زمان یک کاربر به سندی دسترسی یابد CIPRESS کد ناپیدای محرمانه جدیدی که شناسهٔ دسترسی کاربر را در خود دارد به سند می‌افزاید. در مواردی که متن خود حاوی حداکثر مجاز تعداد کد ناپیدا است چرخه جدیدی از اعمال کدهای ناپیدا اعمال می‌شود. یعنی CIPRESS نسخه جدیدی حاوی کد ناپیدای عمومی را از سرویس دهنده محتوا فراخوانی می‌کند. فقط مدیر CIPRESS الگوریتمی که برای خواندن اطلاعات کدهای ناپیدای محرمانه لازم است را می‌داند و بنابراین قادر به تعیین جدیدترین استفاده کنندگان تصویر است. از آنجا که مرکز کلید گزارشی از کسانی که به اسناد دسترسی می‌یابند نگه می‌دارد تمامی کاربران تک‌تک خطوط اسناد قابل شناسایی هستند. کدهای مخفی حتی زمانی که از کامپیوتر خارج شوند و بر روی وسایل یا رسانه‌های دیگری ذخیره شوند در بین اطلاعات اسناد باقی خواهند ماند، این روش می‌تواند در تشخیص کدهای ناپیدا، اغلب انتقالهای متداولی که بر روی اطلاعات قابل انجام است را از سر بگذارند. CIPRESS می‌تواند کدهای مخفی را حتی اگر تصویر به شکل پویش[2] از خروجی چاپی بوده و حتی تا ۹۰٪ تصویر اصلی خراب باشد، یا تصویر به شکل سیاه و سفید[3] تبدیل شده باشد تشخیص دهد.

1 - VPN
2 - Scan
3 - Grayscale

اگر چه فرایند وارد کردن کدهای مخفی نمی‌تواند از توزیع و استفاده غیر مجاز از مواد حق نشر جلوگیری کند ولی می‌تواند راهکار نهایی برای اثبات نقض حق نشر در دادگاه باشد. همچنین در مواردی که یک عنصر داخلی در سرقت اطلاعات درگیر است، این کاربر خرابکار قابل تشخیص بوده و مراحل قانونی بر علیه او قابل اجرا است.



شکل ۲- شمایی از چگونگی وارد کردن کدهای مخفی در اسناد توسط CIPRESS

با ترکیب تمامی تکنیکهای فوق CIPRESS یک محیط ایمن فراهم می‌آورد که تمامی کانال‌های ممکن برای حمله به اطلاعات را پوشش می‌دهد. CIPRESS بین اسناد محلی و ثبت شده تمییز قائل می‌شود. این طبقه بندی بر اساس موارد تکنیکی است که چه نوع رمزگذاری بر سند انجام شده است. در CIPRESS اسناد می‌توانند به صورت سند معمولی یا با پیوند داده‌ای[1] ثبت شود. این طبقه بندی مفهومی، به CIPRESS اجازه می‌دهد که نسخه حق نشر اولیه و ثانویه را در نظربگیرد. در مورد اسناد معمولی CIPRESS فرض می‌کند صاحب سند، حافظ حق نشر محتوای آن سند نیز می‌باشد. بر اساس مفهوم پیوند داده یک کاربر اگر بخواهد اسناد دیگری را در سند خود استفاده کند اجازه چنین کاری به او داده نمی‌شود و بجای این کار او باید از روش مرجع‌دهی استفاده کند. کاربر سپس این اقلام جدید را به عنوان سندهای با پیوند داده‌ای و خود را به عنوان حافظ حق نشر ثبت می‌کند. از آنجا که ترکیب اقلام دارای حق نشر یک کار معنوی است و دارای حقوق مربوط به خودش، این شیوه، روش مناسبی برای رفع مشکلات حق نشر است و هیچ حقی برای فرد ایجاد کننده سند دارای پیوند داده‌ای فراهم نمی‌کند. از آنجایی که اقلام استفاده شده همیشه بعنوان مرجع بیان می‌شود و به سند وارد نمی‌شوند نسخهٔ اصلی این مراجع باید هر زمان که ترکیب آنها قابل دسترسی است در دسترس باشد. این امر عدم امکان فرار از حفاظت‌های حق نشر را تضمین می‌کند.

۲-۱- آموزش الکترونیکی در محیط CIPRESS

مزیت اصلی CIPRESS در آموزش، از این خصیصهٔ آن نشأت می‌گیرد که وقتی در سطح سیستم عامل اجرا شوند امنیت کافی را فراهم می‌کند. بنابراین با هر محیط آموزشی قابل ترکیب است و استفاده از برنامه‌های آموزش الکترونیک بر روی یک کامپیوتر مستقل هیچ مشکلی ایجاد نمی‌کند و به دلیل یکپارچگی محصول نهایی این سیستم با شبکه جهانی، CIPRESS می‌تواند بسرعت با آموزشهای الکترونیکی بر پایه شبکه اینترنت سازگار شود. در این موارد تمامی دانش‌آموزان باید بر روی کامپیوترهایشان در کنار CIPRESS یک مرورگر اینترنت نیز نصب کرده باشند. CIPRESS از ذخیره سازی، بازیابی و تحویل اقلام آموزشی و همچنین ارتباطات معلم و شاگرد مراقبت می‌نماید. منطق کنترل دوره‌های درسی، نگهداری مشخصات استفاده

1 - Data Linkage

کنندگان و دوره‌ها و مدیریت کاربران بایستی توسط یک سیستم خاص آموزشی مثل IDEAL MTS [4] یا در موارد ساده تر توسط یک سرویس‌دهنده اینترنت ساده انجام شود.

۲-۱-۱- کنترل بر استفاده ی اقلام آموزشی در تمام طول عمر این اقلام

در محیط CIPRESS دانش‌آموزان می‌توانند به اقلام آموزشی فقط با داشتن هویت مشخص در این سیستم دسترسی داشته باشند و مرکز کلید، کلید مورد نیاز برای رمزگشائی این اقلام آموزشی را برای این دانش‌آموزان فراهم می‌کند. مورد مهم در اینجا این است که بازیابی کلید فقط یک بار زمانی که اقلام آموزشی تحویل داده می‌شود انجام نمی‌گیرد. بلکه با هر بار دسترسی به این اقلام تکرار می‌شود. از آنجا که دانش‌آموزان نمی‌توانند از مرکز کلید که در یک محیط امن قرار دارد، سوء استفاده کنند در محیط CIPRESS فقط کاربران قانونی می‌توانند به اطلاعات و اقلام آموزشی دسترسی یابند. در نتیجه اطلاعات حساس و محرمانه می‌توانند در اقلام آموزشی گنجانده شوند.

اگر یک متجاوز، این اقلام آموزشی را بدزدد تنها چیزی که به دست می‌آورد، اطلاعات رمزگذاری شده است. برای دیدن محتوای این اطلاعات او نیازمند یک کلید از مرکز کلید است. به همین روش CIPRESS از توزیع مجدد و غیر قانونی اقلام آموزشی موجود در کامپیوتر شخصی دانش‌آموزان نیز جلوگیری می‌نماید. اگر دانش‌آموزی که به صورت قانونی به اطلاعات دسترسی دارد، یکی از اقلام آموزشی را برای دانش‌آموز دیگری بفرستد اطلاعات به شکل رمزگذاری شده انتقال می‌یابد. دانش‌آموز جدید فقط در صورتی می‌تواند به اطلاعات دسترسی یابد که مرکز کلید، کلید مناسب را به او تحویل دهد. از آنجا که کلیدهائی که در CIPRESS استفاده می‌شود برای یک مجموعه سند و کاربر سند، منحصر بفرد است. یک دانش‌آموز نمی‌تواند کلید دانش‌آموز دیگر را مورد استفاده قرار دهد و از طرفی به خاطر وجود رمزگذاری مجدد و وارد کردن کدهای مخفی در اسناد، کنترل بر دسترسی به اقلام آموزش وقتی که به یک دانش‌آموز تحویل شد، پایان نمی‌یابد. در عوض کنترل بر دسترسی بر اقلام آموزشی و اجزای آن‌ها در تمام طول عمر آن سند گسترده شده است و از آنجا که CIPRESS، در درون سیستم عامل وارد می‌شود نه فقط در سیستم آموزشی دانش‌آموزان نمی‌توانند خارج از یک نشست[1] آموزشی از اقلام آموزشی استفاده کنند.

مزیت دیگری اضافه بر امنیت این سیستم این واقعیت است که درCIPRESS مرکز کلید در هر دسترسی به داده‌ها درگیر است و به همین خاطر می‌تواند ردپای فعالیت‌های کاربران را نگه دارد. اطلاعات در مورد استفاده‌های کاربران که توسط مرکز کلید نگهداری می‌شود می‌تواند در موارد زیر مورد استفاده قرار گیرد:

تنظیم کارایی و مدیریت کیفیت: این اطلاعات که چه تعداد دانش‌آموزانی به سیستم دسترسی دارند اطلاعات ذی قیمتی برای تعلیم دهندگان است. زیرا به آنها اجازه می‌دهد تا کارایی نهایی سیستم را بهینه کنند. اطلاعاتی که در یک سند آموزشی در دسترس است و اینکه تا چه میزان دسترسی به آن وجود دارد به مسئولین تعلیم و آموزش کمک می‌کند تا نیازهای مشتریانشان را پوشش دهند و همچنین بینش لازم برای مدیریت کیفیت را نیز فراهم می‌آورد.

حسابداری و ارائه صورتحساب: این مورد به فعالیت‌های دانش‌آموزان مربوط می‌شود از آنجا که مرکز کلید CIPRESS گزارشی از هر کلید تحویل داده شده را نگه می‌دارد همهٔ آن چیزی که برای نگه داشتن حساب و ارائهٔ صورتحساب نیاز است، در مرکز کلید وجود دارد. عملیات حسابداری و ارائه صورتحساب به نحوی که توسط مرکز کلید و در شرایط ایمن انجام می‌شود نیازمند منابع مالی فوق توان شرکت‌ها متوسط و کوچک است. بنابر برای ارائه دهنده‌های سرویس اینترنت[2] یا شرکت‌های ارتباطات راه دور[3] که منابع تکنیکی و مدیریتی محدودی دارند استفاده از مرکز کلید و فرستادن صورت حساب در ازای ارائه خدمات، می‌تواند یک مدل تجاری منطقی باشد. همچنین یک ارائه دهنده سرویس‌های آموزش و پرورش می‌تواند فقط بر روی ایجاد و نگهداری اقلام آموزشی و دیگر سرویس‌های مربوط به یادگیری چون آموزش‌های خصوصی و ارائه مدرک تمرکز

1 - Sessen
2 - ISP
3 - Telecomunication

کند. این مطلب می‌تواند این شانس را برای سرمایه گذاران کوچک و متوسط فراهم کند که یک ارائه دهنده سرویس‌های آموزشی باشند، بدون اینکه متحمل بار زیاد مالی برای گسترش سخت افزار و پرسنل مورد نیاز در حسابرسی شوند. با توجه به تمایز موجود میان سرویس دهندهٔ محتوای سند و مرکز کلید، CIPRESS به خصوص مدل تجاری مناسبی خواهد بود.

نگهداری مشخصات کاربران: آنچنان که قبلا ذکر شد، نگهداشتن مشخصات کاربران باعث افزایش کیفییت دوره‌های آموزشی می‌شود. از آنجا که CIPRESS همه دسترسی‌ها به اقلام آموزشی را چه در زمان آموزش و چه در هر زمان دیگر تشخیص داده و ثبت می‌کند، اگر مشخصات افراد توسط CIPRESS جمع آوری شده باشد می‌توان به اطلاعات دقیقتری در مورد افراد دست یافت.

۲ـ۱ـ۲ـ مزایای جدید در زمینهٔ یادگیری

با اعمال کنترل دائم از طرف صاحب اقلام آموزشی بر تولیداتش، CIPRESS به طور مؤثری از توزیع‌های غیر مجاز این محصولات از طریق دانش‌آموزان جلوگیری می‌کند. این مسئله یک مشخصهٔ بارز برای بازشناخت مفهوم یادگیری در سناریوی عرضه و تقاضاست. در چنین سناریوئی دانش‌آموزان به صورت بالقوه قادرند به هر صحنه از نمایشنامهٔ اقلام آموزشی دسترسی پیدا کنند، ولی فقط برای آن اقلامی که واقعاً استفاده کرده‌اند. صورتحساب پرداخت می‌کنند. دانش‌آموزان دارای این مزیت هستند که می‌توانند به محض نیاز به اقلام آموزشی به آنها دسترسی پیدا کنند بدون اینکه هیچ روال ثبت نامی را انجام دهند. مزیت CIPRESS در این زمینه این است که از هر دسترسی به اطلاعات آگاه است و فارغ از اینکه از چه کانال ارتباطی این دسترسی انجام می‌شود آن را در مرکز کلید حفظ می‌کند. توسط CIPRESS هر نوع از اقلام آموزشی حتی نسخهٔ نهائی برنامه‌ها را می‌توان به روش پرداخت برای هر مورد به کار برد.

استفاده از اقلام آموزشی با محدودیت زمان استفاده: به صورت معمول هر دانش‌آموز پس از اینکه اقلام آموزشی به او تحویل داده شد می‌تواند به آن تا هر زمان که بخواهد دسترسی پیدا کند. توسطCIPRESS صاحب اقلام آموزشی یا سرویس دهنده آموزش و پرورش می‌تواند با تنظیم اجازه نامه‌های CIPRESS در هر زمان که ارده کند باعث شود دیگر مرکز کلید برای هر قسمت خاص از آن سند کلید تولید نکند، به این ترتیب می‌توان تا هر زمانی که دانش‌آموز برای آن سند پول پرداخت کرده است محدوده زمانی دسترسی او را کنترل کرد.

سادگی نگهداری: این مورد در به روز نگه داشتن نرم افزارها بسیار نقش بارزی دارد. فرض کنید که سرویس دهندهٔ آموزشی تصمیم دارد که دیگر استفاده از یک قلم آموزشی منسوخ را مسدود کند که می‌تواند به دلیل ایرادات آن سند یا دلایل قانونی یا سیاسی یا ... باشد. با سیستم‌های مرسوم سرویس دهنده به هیچ طریق نمی‌تواند مطمئن باشد که دانش‌آموزان دیگر به کار با آن اقلام آموزشی که به آنها تحویل داده شده است ادامه نمی‌دهند، چون هیچ وسیله‌ای برای اعمال کنترل ندارند. در حالی که با CIPRESS فقط کافی است حقوق دسترسی با آن سند را به گونه‌ای تنظیم کنیم که دیگر کلیدی برای آن سند ارئه نشود.

تحویل به روش پیشرفته: استفاده از CIPRESS و سیستمها آموزشی بر پایه اینترنت نیازمند اتصال دائم به اینترنت است تا کلیدهای CIPRESS توسط کاربر دریافت و اطلاعات کنترلی ارسال شود. این اطلاعات بسیار کم حجم هستند بنابر این ارسال آنها هیچ تأخیری ایجاد نمی‌کند. مورد دیگردر زمینه تحویل اقلام چند رسانه‌ای به خصوص تصاویر ویدیویی با کیفیت بالاست. در این مورد سرویس دهنده آموزشی می‌تواند ابتدا تصاویر ویدیویی را بر روی لوح فشرده[1] برای دانش‌آموز بفرستد و سپس این تصاویر ویدیویی توسط فایل‌های سیستم بارگذاری می‌شوند و از تأخیرهای طولانی که جریان یادگیری را مختل کرده و هزینه‌های اتصال را زیاد می‌کند جلوگیری شود. وقتی به این روش عمل می‌شود باید اطمینان یافت که دانش‌آموزان نمی‌توانند به محتوای اطلاعات ارسالی توسط لوح فشرده، که می‌تواند سئوال امتحان یا تمرین باشد، قبل از زمان تعیین شده توسط سرویس دهنده دسترسی یابند.

1 - CD

با استفاده از CIPRESS مشکل به سادگی قابل حل است و تمام آن چیزی که باید صاحب سند یا حتی بهتر بگوییم سیستم اتوماتیک آموزشی انجام دهد این است که حقوق دسترسی را تنظیم نماید. وقتی که اطلاعات بر روی لوح فشرده تحویل دانش‌آموز می‌شود او هیچ گونه حق دسترسی به آن اسناد را ندارد، بنابراین هیچ کلیدی دریافت نمی‌کند و به اطلاعات نیز دسترسی ندارد. به محض اینکه دانش‌آموز، لازم است به اطلاعات دسترسی یابد، سیستم، حقوق دسترسی را از طریق ارائه کلید در اختیار او قرار می‌دهد.

سازگاری سیستم با اشخاص: دانش‌آموزان مختلف، گذشته‌های مختلف و اهداف آموزشی متفاوت دارند و ساده‌تر بگوییم برای سطوح متفاوتی از یادگیری و آموزش پول پرداخت می‌کنند. بصورت ایده‌آل می‌توان گفت که یک دانش‌آموز خاص به یک مجموعهٔ خاص از اقلام آموزشی نیازمند است. سرویس دهنده‌های آموزشی باید از یک سو مطمئن باشند که دانش‌آموز به تمام آن چیزهایی که نیاز دارد یا مستحق دانستن آنهاست دسترسی دارد ولی از سوی دیگر نباید اجازهٔ دسترسی به مواردی که به او مربوط نیست را بدهند. وقتی اقلام آموزشی بر روی لوح فشرده تحویل می‌شود عملی نیست که یک لوح برای هر دانش‌آموز تهیه شود. توسط CIPRESS سرویس دهندهٔ آموزشی می‌تواند لوح فشردهٔ حاوی تمامی اطلاعات را که برای همه دانش‌آموزان نیاز است، به صورت رمزگذاری شده تهیه کند، سپس سرویس‌دهنده، کنترل می‌کند که هر دانش‌آموز به چه اقلام آموزشی نیاز دارد، دقیقاً حق استفاده از همان اقلام را به او اعطا می‌کند و همچنین در آینده نیز هیچ مشکلی وجود ندارد که حق استفاده از اقلام بیشتر به او داده شود یا حقوق قبلی او محدود گردد.

۳ـ نتیجه گیری

اگر چه شبکه جهانی اینترنت تمامی امنیت لازم برای یادگیری الکترونیک را پوشش نمی‌دهد راه‌های دیگری برای غلبه بر این مشکلات و رسیدن به یک سطح قابل قبول امنیت وجود دارد.

چارچوب‌های امتحان نشان می‌دهد که چگونه می‌توان مواد امتحانی دارای تعامل زیاد بین امتحان گیرنده و دانش‌آموز را با یادگیری‌های برپایهٔ اینترنت یکپارچه کرد، به طوری که امنیت و اطمینان در کنترل موفقیت دانش‌آموزان تضمین شود. این چارچوب‌ها کاملًا عملیاتی بوده و به سادگی قابلیت سازگاری و توسعه دارند. این چارچوب‌ها می‌توانند به عنوان بستر مناسب در فرآیند امتحان دانش‌آموزان، برای کشف روش‌های جدید یادگیری انجام وظیفه نماید. در اینجا روشهایی که ملزومات شبکه جهانی اینترنت را بهتر بکار می‌برند بیشتر مد نظر است. در محیط‌هایی با مدیریت قابل اطمینان و نظارت مناسبی بر کامپیوترهای شبکه وجود داشته باشد حتی این روش‌ها قادر به جلوگیری از دسترسی‌های غیر مجاز به اقلام آموزشی است.

۴- مراجع

[1] Busch C, Graf F, Wolthusen S, Zeidler A. A system for intellectual property protection. Proceedings of SCI 2000/ ISAS2000, Orlando, USA, July2000.

[2] Koch E, Zhao J. Towards robust and hidden image copyright labeling. Proceedings of the 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Halkidiki, Greece, June 1995. p. 452–5.

[3] Busch C, Funk W, Wolthusen S. Digital watermarking: from concepts to real-time video applications. IEEE Computer Graphics and Applications (Special Issue on Image Security), 1999;19:25 35.

[4] Bork A, Ibrahim B, Milne A, Yoshi R. The Irvine-Geneva course development system. In: Aiken R, editor. Education and society, information processing 92, vol. 2. Amsterdam:Elsevier, 1994.