ISSN: 2538-3787
http://www.Joce.ir

مجله علمی فقه، حقوق و علوم جزا (سال ششم)
شماره ۲۰ /تابستان ۱۴۰۰ / ص ۱۱۳- ۱۰۶

بیومتریک و رمزنگاری در تضمین امنیت اسناد رسمی

امیررضا محمودی[۱]، سیده مهشید میری بالاجورشری[۲]

[۱] دکتری حقوق عمومی، استادیار گروه حقوق دانشگاه آزاد اسلامی واحد لاهیجان-گیلان.

[۲] دانشجوی دوره کارشناسی ارشد رشته حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد لاهیجان- گیلان.

نام نویسنده مسئول:
امیررضا محمودی

تاریخ دریافت: ۱۴۰۰/۳/۸
تاریخ پذیرش: ۱۴۰۰/۵/۳۰

چکیده

سیستم های رمزنگاری و بیومتریک سیستم هایی هستند که به موجب آن ها ویژگی های فیزیکی و رفتاری افراد وسیله ای برای تشخیص هویت آنها می شود. به طوری که تشخیص هویت به موجب ابزار های رایانه ای با پردازش داده های بدن شخص زنده صورت می گیرد. چنین سیستمی امروزه کلیه رمزنگاری های دستی و ابتدایی را دستخوش تغییر قرار داده است و با امنیت بالایی که دارد در همه حوزه های زندگی بشر وارد شده است. وجود چنین سیستمی نه تنها امنیت داده ها و اطلاعات افراد را تضمین کرده است بلکه تبدیل به ابزاری مطمئن در حوزه های بانکی، ثبتی و حقوقی شده است، به طوری که با اجرای آن در این حوزه ها امنیت اسناد صادر شده هم از بعد جعل سنتی و هم از بعد جعل الکترونیک به حداقل رسیده است و وسیله ای برای پیشگیری از سو استفاده های احتمالی شده است.

واژگان کلیدی: بیومتریک، رمزنگاری، امنیت اسناد، پیشگیری از جعل الکترونیک..

ISSN: 2538-3787
http://www.Joce.ir

مقدمه

بشر از ابتدا برای حفظ حریم شخصی خود از ابزارهای مختلفی استفاده کرده است. به عنوان نمونه برای حفظ حریم اختصاصی منزل از کلید استفاده می کند، یا برای محافظت از داده های کامپیوتری خود از رمز های الکترونیکی استفاده می نماید و جهت محافظت از حریم خصوصی فعالیت های بانکی خود از رمز های معمول استفاده می نماید. اینها ابزارهای ابتدایی برای پردازش[۱] و محافظت از حریم خصوصی[۲] اشخاص در فعالیت های روزانه می باشد. اما مشکل آنجاست که امکان دارد کلید گم شود یا رمز مورد فراموشی قرار گیرد، حتی وضعیت زمانی بغرنج می شود که شخصی دیگر کلید و یا رمز را پیدا کرده و مورد استفاده قرار دهد. بنابراین جهت تضمین امنیت حریم خصوصی افراد و همچنین اسناد و جلوگیری از سو استفاده های احتمالی گذر از رمز ها و کلید های سنتی به سمت بیومتریک و رمزنگاری ضرورت دارد.

در این راستا قانون تجارت الکترونیک و ماده ۴۰ قانون جرایم رایانه‌ای و همچنین لایحه صیانت و حفاظت از داده های شخصی مصوب ۱۳۹۷، به استفاده از روش‌های ایمن برای محافظت از داده‌ها[۳] اشاره کرده است به طوری که یکی از مهمترین موارد را بیومتریک و رمزنگاری قلمداد کرده است. فناوری بیومتریک داده‌های اشخاص را بر اساس الگوی عمومی دریافت می کند و مورد پردازش قرار می دهد و فقط به شخصی که داده‌هایش پردازش شده اجازه می دهد که به اطلاعات دسترسی داشته باشد. به بیانی دیگر دیگران اجازه دسترسی به این اطلاعات را ندارند.

رمزنگاری نیز دانش تغییر دادن اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است. به شکلی که تنها شخصی که از کلید و الگوریتم آگاه است می‌تواند اطلاعات اصلی از اطلاعات رمزگذاری را استخراج کند و برای فردی که به این اطلاعات دسترسی ندارد بصورت ناخوانا باقی می‌ماند و بدین صورت داده‌ها از خطر تحریف در امان می‌مانند و می توانند مورد استناد واقع شوند. (موذن زادگان، دهکری، یوشی، ۱۳۹۴، ۶۹)

با وجود نص صریح قوانین و اعلام اعمال و اجرای روش های بیومتریک و رمزنگاری، طرق اعمال این ابزارها و اینکه با چه مکانیزمی به کار گرفته شوند محل ابهام می باشد. همچنین در رابطه با راهکارهای پیاده سازی این ابزارها خلا های قانونی فراوانی موجود می باشد. بنابراین در این مقاله به بررسی چگونگی اعمال مکانیزم های ایمن سازی اسناد الکترونیک با روش توصیفی-تحلیلی و به صورت کیفی خواهیم پرداخت.

---

[۱] . هرگونه عملیات دستی یا خودکار بر داده‌های شخصی،شامل و نه محدود به ایجاد، ثبت، دریافت، گردآوری، نگهداری، جداسازی، تغییر، تجزیه و تحلیل، طبقه‌بندی، ساختاربندی، تطبیق، ذخیره‌سازی، اشتراک‌گذاری، فرستادن، توزیع و عرضه، انتشار و در دسترس قرار دادن و پاک کردن آن‌ها.

[۲] . در قانون اساسی, منشور حقوق شهروندی و قانون آزادی اطلاعات به صورت اجمالی به حریم خصوصی اشاره شده است. در اصول ۲۲ و ۲۳ و ۲۵ قانون اساسی به ترتیب مصونیت از تعرض, منع تفتیش و تجسس در حریم خصوصی اشخاص بیان شده است. در منشور حقوق شهروندی, ابتدا در ماده ۱۳ ممنوعیت تعرض به حریم خصوصی مطرح و در ماده ۳۵ به حفاظت از داده ای شخصی اشاره کرده است و امنیت اطلاعات در فضاهای سایبری را از حقوق مسلم شهروندان می داند و نهایتا به شرح کامل حریم خصوصی از مواد ۳۶ الی۴۲ پرداخته که مشمول محل سکونت, اشیاء خصوصی, نامه های الکترونیکی و غیر الکترونیکی, ارتباطات تلفنی و ... می گردد و همچنین احترام به این حقوق حتی در رسانه ها و تریبون ها را نیز الزامی می داند و در ماده ۸۲ حتی گزینش و اشتغال افراد از روش های ناقض حریم خصوصی را نیز، ممنوع کرده است. در قانون آزادی اطلاعات, در فصل چهارم, استثنایات دسترسی به اطلاعات بیان شده که برخی از آن عبارتند از اسراردولتی, حریم خصوصی مصرح در قانون مگر اینکه دارنده آن اذن انتشار آن را پیشاپیش داده باشد یا خواهان اطلاعات ولی, قیم یا وکیل او باشد و همچنین تهدیدی بر امنیت و آسایس عمومی محسوب گردد. در ماده ۱۴ همان قانون مستقیما اشاره به حریم خصوصی, اطلاعات تحصیل شده از روش های ناقص حریم خصوصی نموده و آن را ممنوع کرده است.

[۳] . داده ها در فناوری اطلاعات به دو گونه تقسیم می شود:

الف: داده شخصی عبارت است از داده ای که به تنهایی یا به همراه داده های دیگر،مستقیم یا غیر مستقیم شخص موضوع داده را از طریق ارجاع به یک شناسه می‌شناساند.

ب: داده شخصی حساس عبارت است از داده شخصی که ریشه قومیبا قبیله ای، نظرات سیاسی، مذهبی وفلسفی، مشخصات وراثتی یا اطلاعات سلامت شخص موضوع داده را آشکار می سازد.

ISSN: 2538-3787
http://www.Joce.ir

الف: تعریف بیومتریک

بیومتریک در زمینه فناوری اطلاعات از فناوری‌های نوظهور می باشد. واژه بیومتریک از زبان یونانی سرچشمه گرفته و از دو بخش «به یو» به معنی زندگی و «متریک» به معنی اندازه‌گیری تشکیل شده است. (عسگرزاده، ۱۳۹۵، ۱۴) بیومتریک در اصطلاح به مجموعه روش های خودکار تشخیص یا تأیید هویت یک موجود زنده از طریق اندازه گیری مشخصات و خصوصیات فیزیولوژیکی یا رفتاری منحصر به فرد و متمایزکننده آن موجود گفته می شود. در نتیجه بیومتریک یک مجموعه فناوری به حساب می آید. (پورمیدانی، ۱۳۹۶، ۱۲)

این فناوری داده‌هایی از افراد را با توجه به الگوی عمومی و بطور خودکار دریافت می‌نماید و آن را پردازش و تحلیل می کند تا افراد را در جامعه آماری بزرگتر از هم متمایز کند و از جعل یا سرقت اطلاعات و یا دسترسی غیرمجاز به اطلاعات اشخاص و داده‌ها جلوگیری کند و امنیت افراد را تامین نماید.

۱: مصادیق بیومتریک در قلمرو امنیت اسناد و داده ها

خصوصیات بیومتریک به طور کلی به دو دسته تقسیم می‌شوند: خصوصیات فیزیولوژیکی و خصوصیات رفتاری. در رابطه با خصوصیات فیزیولوژیکی، این خصوصیات مربوط به ساختار و شکل بدن می‌باشد. شناسایی از طریق چهره‌نگاری، اثر انگشت، شبکیه نگاری، عنبیه نگاری، نقشه‌ی کف دست، نقشه‌ی رگ‌های دست، صورت، ساختار ناخن، شکل گوش و هندسه‌ی دست نمونه‌هایی از این روش می‌باشند. در رابطه با خصوصیات رفتاری، بعضی از رفتارهای افراد مانند چگونگی راه رفتن، تشخیص لبخند، امضا و نحوه تایپ کردن نمونه‌هایی از این روش می‌باشند. (احمدی، ۱۳۸۸، ۱۴)

سیستم بیومتریک در واقع نرم‌افزار یا سخت‌افزار کامپیوتری می‌باشد که برای بررسی و شناسایی افراد استفاده می‌شود. از جمله مواردی که بیومتریک در آنها کاربرد دارد می‌توان اشاره کرد به: گواهینامه‌های رانندگی، تراکنش‌های مالی و اعتباری، تایید هویت مشتریان و دسترسی به حساب‌ها، رأی‌گیری، شناسایی مجرمان، شناسایی شهروندان، کارت‌های شناسایی، مدیریت بحران‌های بزرگ شهری، تراکنش‌های از راه دور مثل تجارت الکترونیک، دسترسی به رایانه‌های شخصی یا شبکه و حفاظت از داده‌ها و سیستم‌های رایانه‌ای. در این میان مهم‌ترین کاربرد بیومتریک ایمن‌سازی سند الکترونیک می‌باشد. (حسن‌آبادی، ۱۳۸۶، ۱۵)

۲: مزایای بیومتریک

مزایای بیومتریک عبارتند از: افزایش راحتی، افزایش ایمنی، کاهش تقلب و دسترسی غیر مجاز و تشخیص افراد مظنون. سیستم‌های بیومتریکی دستیابی به اطلاعات مورد نظر را بسیار سریع‌تر می کند. همچنین باعث کاهش هزینه‌های مربوط به مسائل امنیتی و نگه‌داری دستگاه‌ها می‌شود. (هاتف، ۱۳۸۶، ۷۲)

تعداد زیادی از کاربران به خاطر سخت بودن به یاد سپردن کلمات یا اعداد، رمز عبور خود را ساده انتخاب می کنند و یا در جایی می‌نویسند.در چنین شرایطی کدها و رمزهای عبور ممکن است به سادگی حدس زده شود یا قابل شکستن باشد. اما بیومتریک‌ها نیاز به نگه‌داری خاصی ندارند و همچنین قابل فراموشی یا سرقت نمی‌باشند. (همان، ۷۲)

بیومتریک‌ها باعث جلوگیری از تقلب افراد سودجو در انجام امور مالی، ورود به مراکز امنیتی، استفاده از منافع عمومی و... می‌شوند. (همان، ۷۳) بیومتریک‌ها هویت واقعی افراد را مشخص می‌کند. در نتیجه باعث جلوگیری از اعمال تروریستی، مهاجرت‌های غیرقانونی و فرار از قانون می‌شود.

۳: بیومتریک و ایمن‌سازی اسناد الکترونیک

بیومتریک قادر است خصوصیات یک شخص را بدون تماس پیوسته کارمند با سیستم ارزیابی و اندازه‌گیری نماید و در راستای تامین امنیت اطلاعات بسیار مفید باشد. بیومتریک با محافظت کردن از اطلاعات هویت افراد تضمین کننده‌ی یکپارچگی امنیت است و برای حمایت از این حیطه مهم ترین فاکتور می‌باشد. مثلا اگر شخصی کارت هوشمندش را گم نماید و یک بیگانه آن را بیابد نتیجه‌اش به خطر افتادن سابقه‌ی اعتباری آن شخص است؛ اما اگر کارت هوشمند را فقط زمانی بتوان استفاده کرد که کاربر مورد نظر از طریق خصوصیات بیومتریک خود شناسایی گردد در چنین شرایطی کاربر از این گونه خطرات و تهدیدها در امان است. (ساجدی، ۱۳۸۶، ۱۴۰)

ISSN: 2538-3787
http://www.Joce.ir

سامانه‌ی بیومتریک اطلاعات کاربران را فقط در اختیار افراد مجاز قرار می‌دهد و دسترسی افراد غیرمجاز به این اطلاعات را محدود می‌سازد. برای این کار بیومتریک در سه مرحله عمل می کند: "جمع‌آوری، استخراج، مقایسه". (موذن زادگان، دهکری، یوشی، ۱۳۹۴، ۸۸) در مرحله اول سیستم باید بیومتریکی را که می‌خواهد مورد استفاده قرار بگیرد را جمع‌آوری کند. همه‌ی سیستم‌های بیومتریک دارای نوعی سازوکار جمع‌آوری می‌باشند. این سازوکار می تواند به شکل‌های مختلفی باشد مثلا: یک دوربین که تصویری از صورت یا چشم می گیرد، یک حسگر که فرد انگشت یا دست خود را بر روی آن می گذارد و یا نرم‌افزاری که سرعت و نحوه تایپ کردن را ثبت می‌نماید. (ساجدی، ۱۳۸۶، ۱۶۹) در مرحله دوم شاخصه‌های معینی از بیومتریک استخراج می‌گردد و از این طریق فقط صفات تعیین شده‌ای جمع آوری می شوند. برای مثال نقاط فشار روی امضا یا اندازه‌های معینی از اثر انگشت. با توجه به نوع بیومتریک و طراحی سیستم مشخص می شود که کدام یک از قسمت‌ها مورد استفاده قرار می گیرند.[۴] (همان، ۱۷۰) در مرحله سوم که مرحله مقایسه است، سیستم بیومتریک شاخصه‌های تعیین شده‌ای از خصوصیات بیومتریک یک شخص را می‌سنجد و هر دفعه که آن شخص بیومتریک زنده خود را عرضه می‌نماید، ثبت می کند. (همان، ۱۷۲)

اطلاعاتی که استخراج گردیده به کد تبدیل می‌شوند از طریق شیوه‌ای که نمونه ایجاد شد. این کدهای جدیدی که از روی اسکن زنده تشکیل شده در صورت تطبیق یکی با یکی، با یک نمونه واحد ذخیره شده مقایسه می گردد. این تطبیق و مقایسه اگر در طیف معینی از رقم‌های آماری به طور صحیح عمل کند، در سیستم معتبر دانسته می‌شود. هر دفعه که یک سیستم بیومتریک چهره، صدا، امضا یا اثر انگشت یک فرد را می خواند، ممکن است داده‌های متفاوتی را ایجاد کند. نرم‌افزار تشخص اگر برای این نوسان جواب‌گو نباشد، به فرد اجازه وارد شدن نمی دهد. بیومتریک یک لایه محافظتی که با کلمات رمز استاندارد اقدام می‌شود تشکیل می دهد و فقط به شخصی که صاحب این اطلاعات بیومتریکال است اجازه‌ی وارد شدن می دهد. (موذن زادگان، دهکری، یوشی، ۱۳۹۴، ۸۷)

بدین صورت بیومتریک سه لازمه‌ی مهم برای وارد شدن به دنیای سایبر را ایجاد می کند: شناسایی هویت، تایید هویت و امنیت هویت. شناسایی هویت یعنی به یک شخص خاص شناسه نسبت داده شود، سیستم بیومتریک به راحتی هویت فرد را افشا می‌کند. تایید هویت یعنی اینکه هویت ادعا شده از سوی شخص توسط دیگران تصدیق شود. امنیت هویت هم به معنای محافظت کردن از سیستم‌های اطلاعاتی در برابر ورود افراد غیرمجاز است. (همان، ۸۷)

با توضیحاتی که داده شد مشخص می شود که سیستم بیومتریک به صورت چند لایه اطلاعات را پردازش می کند، به طوری که هر کدام از لایه ها برای بقیه لایه ها الزامی می باشند و بدون وجود هر یک از آنها اجرای عملیات به کلی متوقف می شود. لازمه اجرای این سیستم در بدنه حوزه اداری و اجرایی کشور نیازمند بسترسازی های متعددی است که همه آنها در راستای همدیگر فعالیت کنند. ثبت احوال متمرکز، ثبت اسناد متمرکز، سامانه های قضایی و اداری متمرکز و سیستم بانکی متمرکز به همراه هم و با همکاری هم می توانند از فرایند احراز هویت بیومتریک استفاده کرده و راه را برای هرگونه سو استفاده و جعل و دور زدن قانون تنگ تر کنند. به طوری که با ثبت یک سند تمامی سیستم های مرتبط بتوانند آن را رهگیری نمایند و بتوانند تشخیص دهند که در چه تاریخی چه عملیاتی توسط فرد مورد نظر صورت گرفته است. وجود بیومتریک همچنین راه را برای دور زدن های قانون که معمولا با بدست آوردن مدارک می تواند صورت گیرد را نیز می گیرد.

ب: رمزنگاری

رمزنگاری دارای تاریخچه ای بسیار طولانی است.[۵] به زبانی ساده رمزنگاری فرایند محافظت از یک داده یا فایل به وسیله رمز است. به طوری که با عملیاتی شدن رمز صرفا فرد خاصی توانایی دسترسی به آن فایل و داده را خواهد داشت. عملیات رمز

---

[۴] . به این اطلاعات استخراج شده داده‌های خام نیز گفته میشود که تبدیل به یک سری کد ریاضی می‌گردند. این کدها به صورت نمونه ذخیره میشوند. در سیستم‌های مختلف نحوه انجام این کار متفاوت است. مجموعه واحدهای سخت‌افزاری یا برنامه‌های نرم‌افزاری یک سیستم معین می کند که ذخیره شدن این اطلاعات به چه صورت باشد.

[۵] . در یونان باستان، از ابزاری به‌نام برای رمزنگاری آسان پیام‌ها به روش رمزنگاری جابه‌جایی استفاده می‌شد. رمزنگاری جابه‌جایی با تغییر حروف یک پیام و جابه‌جا کردن آن‌ها انجام می‌شود .پیام‌هایی که به‌کمک رمزنگاری ارسال می‌شدند، حتی درصورت کشف توسط افراد دیگر و باز شدن، قابل خواندن و

ISSN: 2538-3787
http://www.Joce.ir

گذاری در قدم اول با به هم ریختن داده های ورودی[۶] صورت می گیرد و سپس گیرنده داده های مزبور را با استفاده از یک رمز از وضعیت بهم ریخته خارج ساخته و آن را به حالت رمز گشایی[۷] می رساند.

رمزنگاری کردن فایل‌ها و اطلاعات مهم از جرایمی مانند دسترسی غیرمجاز به اطلاعات جلوگیری می کند و راه حل بسیار مناسبی برای پیشگیری از سرقت هویت و محافظت از اطلاعات می‌باشد. رمزنگاری دارای پیشینه طولانی است و کشورها برای محرمانه نگه داشتن اطلاعات مهم به ویژه در زمان جنگ از تحلیل رمز نگاری[۸] آن بهره می‌برند. (بهاری، ۱۳۹۷، ۶۱)

رمزنگاری با استفاده از ریاضیات، داده را به گونه‌ای نگه‌داری می کند که فقط کسانی که مجاز هستند، به اصل داده‌ها دسترسی داشته باشند و از دست‌یابی افراد دیگر و یا حمله‌کننده‌ها جلوگیری می کند. یک سیستم رمز دارای سه رکن اساسی می باشد:

- سازوکار رمزنگاری که از طریق الگوریتم ریاضی متن اصلی را به متن رمزنگاری شده تبدیل می کند؛
- سازوکار کشف رمز که از طریق یک الگوریتم متن رمزنگاری شده را به متن عادی قبلی باز می‌گرداند؛
- سازوکاری برای تولید و پخش کلیدها. (همان، ۷۰)

۱: روش‌های رمزنگاری در امنیت اسناد

برای محافظت از اطلاعات در رمزنگاری، اطلاعات به حالت درهم تبدیل می‌شود و با یک کلید از شکل محرمانه خارج می‌گردد و فقط برای کسی که کلید را دارد خواناست. این متن درهم‌سازی شده متن سری نام دارد. فرایند تشکیل متن سری را سری سازی یا رمزسازی می‌گویند. (عابدینی، ۱۳۹۳، ۱۱۲)

رمزنگاری شیوه‌های مختلفی دارد مانند: پنهان‌سازی، الگوریتم‌های ریاضی، سیستم ابزاری، کدهای منبع، جایگزینی و جابجایی. بیشتر رمزها با جایگشت و جانشینی ایجاد می‌گردند. در جایگشت کاراکترها یا بیت‌ها ترتیب قرار گرفتن‌شان عوض می شود اما در جانشینی کاراکترها یا بیت‌ها جانشین کاراکترها یا بیت‌های دیگر می شوند. (همان، ۱۱۴) ضمنا در این میان رمزنگاری متقارن و رمزنگاری نامتقارن دو نوع از سیستم‌های رمزنگاری هستند:

۱-۱: رمزنگاری متقارن

این روش رمزگذاری به روش تک کلید مشهور می‌باشد. در این نوع رمزنگاری هر دو طرف ارتباط کلید یکسانی را مورد استفاده قرار می‌دهند. بنابراین هر کدام از کامپیوترهایی که در این فرایند تبادل اطلاعات مشارکت دارند باید کلید رمز مشابه‌ای برای رمزگشایی اطلاعات داشته باشند. محتوای فرستاده شده با همان کلیدی که رمز شده است رمزگشایی می‌شود. (بهاری، ۱۳۹۷، ۷۴)

مزایای رمزنگاری متقارن عبارت است از: سرعت بالای این نوع رمزنگاری و کاربرد آن برای حجم زیاد اطلاعات. از معایب رمزنگاری متقارن می توان به موارد زیر اشاره کرد:

- احتمال دسترسی غیرمجاز به کلید زیاد است چون هر دو طرف کلید یکسانی دارند؛
- از آنجایی که فرستنده و گیرنده کلیدهای یکسانی دارند، هر کدام از آن‌ها ممکن است ادعا کنند که طرف مقابل امضاکننده می‌باشد؛
- اگر در ازای هر دو نفر پیام محرمانه باشد ممکن است تعداد کلیدها بسیار زیاد شوند. (وافری، ۱۳۹۲، ۶۳)

تفسیر نبودند. البته چنین سبکی از رمزنگاری با کمی تلاش قابل رمزگشایی بود. به‌هرحال این روش، به‌عنوان اولین روش رمزنگاری در تاریخ شناخته می‌شود. جولیوس سزار، روشی اختصاصی برای رمزنگاری ابداع کرد که به رمز سزار هم مشهور شد. در این روش که از ساده‌ترین راهکارهای رمزنگاری محسوب می‌شود، هر حرف الفبا را به تعداد مشخص به سمت راست یا چپ فهرست حروف جابه‌جا می‌کنند .

[6]. Encrypt.

[7]. Decrypt.

[۸] . علم مطالعه‌ی رمزها و سیستم‌های رمزنگاری. در کاربردهای مجرمانه با استفاده از این علم می‌توان پس از کشف نقاط ضعف سیستم رمزنگاری، بدون داشتن کلیدها به داده‌ی اصلی دسترسی پیدا کرد. در قدیم روشی به‌نام تحلیل تناوب کاربرد داشت که با پیدا کردن تکرار برخی از حروف در پیام‌ها، پیام اصلی را به‌نوعی استخراج می‌کرد. البته روش مذکور در مقابله با الگوریتم‌های مدرن امروزی کارایی چندانی ندارد.

ISSN: 2538-3787
http://www.Joce.ir

۱-۲: رمزنگاری نامتقارن

در رمزنگاری نامتقارن از دو نوع کلید عمومی و خصوصی استفاده می‌گردد و هر فرد دارای یک جفت کلید یعنی کلید عمومی و کلید اختصاصی می‌باشد. کلید اختصاصی محرمانه است اما کلید عمومی می‌تواند در اختیار همه قرار داشته باشد. ارسال کننده پیام را از طریق کلید عمومی رمز می‌نماید و دریافت کننده از طریق کلید خصوصی خود پیام را رمزگشایی می کند. (عابدینی، ۱۳۹۳، ۹۷)

مزایای رمزنگاری نامتقارن عبارت است از: متفاوت بودن کلیدها، حفظ یکپارچگی، اعتبار، صحت و انکارناپذیری اطلاعات، توانایی مقیاس پذیری. از جمله معایب این روش می توان اشاره کرد به پایین بودن سرعت در حجم زیاد اطلاعات و پیچیده بودن ایجاد کلید. (همان، ۱۰۱)

تفاوت رمزنگاری متقارن و نامتقارن در این می‌باشد که در رمزنگاری متقارن برای رمزگذاری و رمزگشایی از کلید یکسانی استفاده می‌شود و کلید رمزگشایی به آسانی از کلید رمزگذاری قابل استخراج است. اما در رمزنگاری نامتقارن برای رمزگذاری و رمزگشایی از کلیدهای متفاوتی استفاده می‌شود و کلید رمزگشایی قابل استخراج از کلید رمزگذاری نیست. (همان، ۱۰۲)

۲: رمزنگاری و کیفیت ایمن‌سازی سند الکترونیک

در رمزنگاری سه سرویس امنیتی وجود دارد:

- محرمانه سازی هویت؛
- اعتبارسنجی مبدأ اطلاعات؛
- عدم ایجاد تغییر در اطلاعات؛

رمزنگاری روش‌های مختلفی دارد. یکی دیگر از این روش‌ها امضای دیجیتال می‌باشد که توسط کاربست کلید خصوصی رمزنگاری می‌شود. این امضا توسط دریافت کننده یا شخص ثالث مستقل می‌تواند تأیید گردد و نیز قابل جعل نمی‌باشد. در صورت حذف حتی یک بیت از داده‌ها، امضا در فرایند اعتبارسنجی رد می‌گردد. در واقع این امضاها نشان دهنده اعتبار منبع یک متن هستند. (موذن زادگان، دهکری، یوشی، ۱۳۹۴، ۸۷) امضای دیجیتالی امنیت را در موارد زیر تأمین می‌کند:

- تصدیق هویت: گیرنده از هویت فرستنده اطمینان پیدا می‌کند؛
- امانت‌داری: اطلاعات در مسیر انتقال مورد دستبرد قرار نمیگیرند و تغییر نمی کنند؛
- غیرقابل انکار بودن: ارسال‌کننده نمیتواند منکر ارسال پیام و امضای داده شود؛
- محرمانه بودن: اطلاعات پیام‌ها محرمانه می‌شوند و فقط برای ارسال کننده و دریافت کننده پیام قابل فهم می‌باشند. (همان، ۸۹)

با توضیحات فوق مشخص می گردد که در حوزه های اداری و اجرایی عملیات رمزنگاری نیز دارای لایه های مختلفی است و فقدان یکی از لایه ها موجب توقف عملیات می گردد. لذا از ملزومات عملیات رمزنگاری علاوه بر بستر سازی های اساسی در کل جامعه و ایجاد سیستم های یکپارچه اطلاعاتی وجود سیستم های سخت افزاری و نرم افزاری پیشرفته لازم و ضروری است. وجود ابزارهای پیشرفته و حساسی که بتواند هویت را تشخیص دهد و پردازش نماید.

نتیجه

امروزه صحبت از دولت الکترونیک، تجارت الکترونیک و بانکداری الکترونیک لزوم بحث و بررسی فرایند های بیومتریک و رمزنگاری را بیش از بیش ضروری کرده است. چرا که اصلی ترین رکن اجرای هر خدمت الکترونیک، تضمین امنیت حریم خصوصی اشخاص می باشد. به طوری که بدون وجود مکانیزم های حفظ حریم شخصی اجرای خدمات الکترونیک موجبات دور زدن قوانین و سو استفاده های فراوان و از بین رفتن حقوق اشخاص را بدنبال دارد.

رمزنگاری به عنوان روشی ساده تر از بیومتریک از زمان اجرای بانکداری الکترونیک و با تاسیس باجه های خودپرداز در جامعه پیاده شده است و شکل پیشرفته آن به صورت امضای الکترونیک در جامعه رواج پیدا کرده است که توانسته در امور مربوط به قوه قضاییه و امورات گمرکی مورد استفاده قرار گیرد.

ISSN: 2538-3787
http://www.Joce.ir

بیومتریک نیز با مطرح شدن دولت الکترونیک زیر ساخت های آن به صورت ابتدایی توانسته است در جامعه گسترش یابد. نمونه بارز آن در در سازمان ثبت اسناد و املاک به کار گرفته شده است. به طوری که امروزه برای ثبت سند به وسیله ابزاری و با گرفتن اثر انگشت فرایند احراز هویت صورت می گیرد.

برای گسترش اجرای فرایند رمزنگاری و بیومتریک در تمامی عرصه ها ابتدا لازم است که زیر ساخت های متمرکز در ثبت احوال نهادینه شود. ثبت اطلاعات اشخاص و راه اندازی کارت های ملی الکترونیک و گسترش سیستم های سخت افزاری شناسایی الکترونیک کارت های ملی و همچنین اتصال سیستم اصلی ثبت احوال به سیستم جامع ثبت اسناد و املاک و همچنین اداره آمار و اطلاعات و برابر سازی سیستم قوه قضاییه و بانکداری لوازم ابتدایی گسترش فرایند بیومتریک و رمزنگاری پیشرفته می باشد. در همین راستا بایستی قوانین نیز به شکل موازی و با پیشرفت چنین سیستم هایی استاندارد سازی شده و نواقص و خلا های آن برطرف شود، به طوری که هر ارگان و سازمانی اصول و روش جداگانه ای جهت اجرای آن ها پیاده نکرده و سلیقه ای عمل نکنند.

ISSN: 2538-3787
http://www.Joce.ir

منابع و مراجع

[۱] بهاری، امین. (۱۳۹۷). آشنایی با مفاهیم بنیادی سیستم‌های رمزنگاری و امنیت شبکه، تهران: نشر سخنوران.
[۲] پورمیدانی، مسعود، (۱۳۹۶). تکنولوژی بیومتریک، اصفهان. انتشارات پورمیدانی.
[۳] عسگرزاده، حسن. (۱۳۹۵). بیومتریک در امنیت اطلاعات، تهران: نشر رویش جوانه های فردا.
[۴] احمدی، جواد. (۱۳۸۸). «دنیای بیومتریک». ماهنامه‌ی فناوری، شماره ۱۳، سال چهارم، صص ۲۸-۱۳.
[۵] حسن آبادی، مهدی. (۱۳۸۶). «تکنولوژی‌های تصدیق هویت». نشریه‌ی رایانه، شماره ۱۶۷، سال دهم، صص ۲۵-۹.
[۶] ساجدی، حامد. (۱۳۸۶). «بیومتریک در خدمت امنیت». دو ماهنامه تکفا، شماره هفت، سال پنجم، صص ۱۴۲-۱۳۴.
[۷] موذن زادگان، حسن‌علی، دهکری، الهام، یوشی، مهشید. (۱۳۹۴). «حفظ صحت و استناد پذیری اسناد الکترونیک با استفاده از بیومتریک و رمزنگاری». پژوهش حقوق کیفری، شماره ۱۲، سال چهارم، صص۹۷-۶۹.
[۸] هاتف، مهدی. (۱۳۸۶). «بیومتریک رویکردی نوین در تأمین امنیت». ماهنامه‌ی توسعه‌ی انسانی پلیس، شماره ۱۲، سال چهارم، صص ۸۴-۷۰.
[۹] عابدینی، فاطمه. (۱۳۹۳). ارائه یک روش جدید برای رمزنگاری بیومتریک. پایاننامه کارشناسی ارشد رشته نرم‌افزار، دانشگاه آزاد اسلامی واحد محلات.
[۱۰] وافری، الهه، (۱۳۹۲). ارایه الگوریتم رمزنگاری تصاویر کارت ملی مبتنی بر نظریه آشوب. پایاننامه کارشناسی ارشد رشته الکترونیک، دانشگاه آزاد اسلامی واحد تهران مرکز.