بانکداری

مدل‌سازی اعتماد در بانکداری اینترنتی

محمود درودچی– استادبخش کامپیوتر دانشگاه کاردینال استریچ امریکا (Mdoroodchi@gmail.com)
آزاده ایرانمهر– دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه شیراز (Iranmehr@gmail.com)

بخش دوم

اشاره

در بانکداری اینترنتی، ریسک از بین رفتن امنیت بسیار زیاد است، زیرا داده‌های حساس مالی در حال نگهداری و ردو بدل شدن می‌باشند و به همین علت، کمبود اعتماد نسبت به امنیت و محرمانگی تراکنش‌های بانکی از طریق اینترنت، یکی از موانع مهم در راه استفاده گسترده مردم از بانکداری اینترنتی است.

در بخش قبلی این مقاله، ضمن مروری بر موضوع اعتماد و بانکداری اینترنتی، به آنالیز گردش اطلاعات در بانکداری اینترنتی و ریسک‌های موجود پرداختیم و یادآور شدیم که مدل‌سازی اعتماد در هر سازمان و موقعیتی، با سازمان و موقعیت دیگر فرق دارد. اینک توجه شما را به ادامه بحث درباره چگونگی ایجاد اعتماد در بانکداری اینترنتی جلب می‌کنیم.

بانک و اقتصاد

ایجاد اعتماد در بانکداری اینترنتی

براساس تهدیدها و ریسک های بدست آمده از آنالیز گردش اطلاعات و ریسک های ناشی از رویکرد تجاری خود بانک ها، می توان مدلی را جهت برقراری و حفظ اعتماد در بانکداری اینترنتی ایجاد کرد.

اگر چه بیشتر سایت های بانکداری اینترنتی اظهار می‌دارند که قابل اعتماد هستند و مشتریان باید تراکنش های مالی با بانک خود را بدون هیچ گونه ترسی انجام دهند، اما ادعای بانک ها به تنهایی برای جلب اعتماد مردم کافی نیست. در واقع، تجربه گذشته مشتری بر روی آن وب سایت یا وب سایت های مشابه، همراه با دانش مشتری در مورد بانک و یا خدمات و محصولات مورد علاقه و هم چنین احساسات وی نسبت به آنچه بر روی صفحه وب می‌بیند، همگی در انجام تراکنش مالی به صورت آنلاین تأثیر دارند. بنابراین، پرسشی که مطرح می شود، این است که چگونه یک وب سایت مشتری را متقاعد می کند که قابل اعتماد است؟

در این قسمت، اجزای مختلفی را که باعث افزایش اعتماد در وب سایت های بانکداری اینترنتی می‌شوند - چه از نظر تکنیکی و فنی و چه از نظر تجاری و روانشناسی- مرور می کنیم.

۱)تراکنش مشتری و بانک: در بانکداری اینترنتی، وقتی مشتری وب سایت مربوطه را مشاهده می‌کند، اولین چیزی که با آن مواجه می شود و بر او تأثیر می گذارد و باعث اعتمادش می شود، واسطه کاربر (User Interface) آن وب سایت است. مواردی مثل محلی سازی، قابلیت کنترل کاربر و خدمات پشتیبانی مشتری هم دارای تأثیر زیادی بر روی ایجاد اعتماد و رضایت مشتریان از خدمات بانکی می‌باشند. تمام فاکتورهای مؤثر بر تراکنش مشتری و بانک در زیر لیست شده اند:

۱-۱)ساختار و محتوای اطلاعاتی سایت: ساختار نامرتب و محتوای ناقص و غیر ساخت یافته یک سایت که نشانه بی دقتی صاحبان آن می‌باشد، اعتماد بازدید کنندگان آن را کم می‌کند، اما برعکس، در صورتی که محتوا، محصولات و خدمات یک وب سایت، به روز و صحیح و قابل فهم باشند، باعث ایجاد حس اعتماد و استقلال در مشتریان می شوند [۲].

بنابراین، برای ایجاد اعتماد نسبت به ساختار اطلاعاتی هر سایت، باید به جنبه های زیر توجه کنیم[۹]:

* باید دید کلی و هدف سایت مطرح شده باشد.
* باید نوع و منبع اطلاعات، بینندگان آن و تاریخ آن دقیقا مشخص شده باشد.
* باید سرویس ها و اطلاعات ارایه شده در سایت، به خوبی تشریح شده باشند.
* باید دستورالعمل هایی برای استفاده از وب سایت و امکانات آن موجود باشد.
* نمایش هشدارهای مناسب برای مواردی که کاربر نخواهد به اطلاعات غیر مجاز دسترسی یابد، ضروری است.
* مالک و صاحب دارایی وب سایت و شرایط استفاده از لینک ها و اطلاعات باید بر روی سایت ذکر شده باشد.
* محتوای وب سایت باید متناسب با هدف بانک و نیاز

اگر چه بیشتر سایت‌های بانکداری اینترنتی اظهار می‌دارند که قابل اعتماد هستند، ولی ادعای بانک‌ها به تنهایی برای جلب اعتماد مردم کافی نیست.

مشتریان باشدو نشانگر تعصبات بیجا نباشد.

* محتوا باید تنها شامل اطلاعات ضروری و مفید باشد و مقدار آن نیز متناسب باشد.

* بیشتر اطلاعات باید مستقیم باشند تا غیر مستقیم و مبهم.

* زبان وب سایت باید واضح و ثابت و متناسب با مشتریان باشد.

* محتوای سایت باید به روز باشد.

* باید حداکثر هر سه ماه یک بار، صفحات مورد بازنگری قرار گیرند.

* باید تاریخ آخرین به روز رسانی و بازنگری در سایت مشخص باشد.

۱-۲) محلی‌سازی سایت: مشتریان معمولاً خصوصیاتی مثل جنس، سن، علایق، زبان و شغل خود را در سایت‌های بانکداری اینترنتی وارد می‌کنند. بانک ها هم با استفاده از این خصوصیات، قادر به شناسایی جمعیت مورد نظر خود خواهند بود و در نتیجه، با توجه به خصوصیات و دیدگاه مشتریان خاص، محتوا و ساختار وب سایت را متناسب با آن طراحی می‌کنند.

ساختار سایت بر مبنای مشتری، به بانک ها این اجازه را می‌دهد که به محتوا، گزینه‌های انتخابی و حتی بنرهای تبلیغاتی مرتبط با مشتری و شخصی سازی شده توجه داشته باشند و با پیش بینی پاره‌ای از خصوصیات و اخلاقیات آنها، بهتر بتوانند احتیاجات مشتریان را برآورده کنند[۱].

در صورتی که سایت به گونه‌ای مشتری محور طراحی شود، ناوبری سایت هم آسان می شود و رضایت مشتریان را افزایش می‌دهد که خود باعث افزایش اعتبار بانک‌ها و ایجاد اعتماد در مشتریان نسبت به آنها می‌شود.

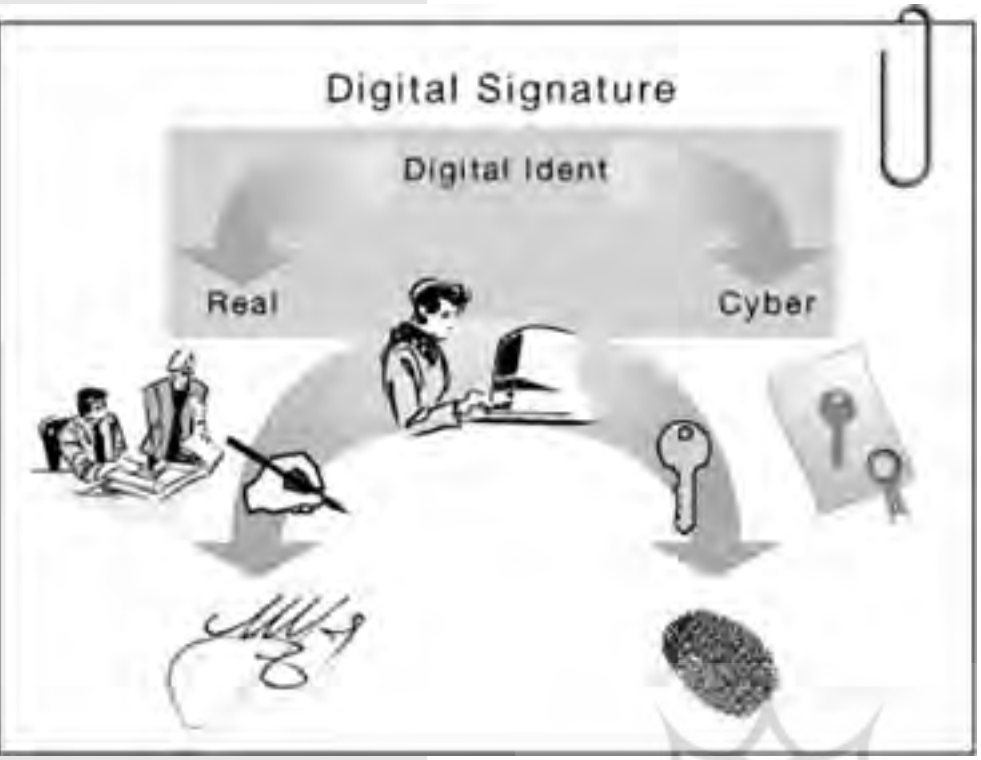
۱-۳)کنترل کاربری: حجم اطلاعات قابل دسترس و دسترسی به آن اطلاعات بر روی وب سایت، نکته مهمی جهت تعیین چگونگی کنترل تراکنش های بانکی از جانب مشتریان می‌باشد. هر چه یک وب سایت کنترل کاربری بیشتری را در اختیار مشتریان قرار دهد، آنها احساس اعتماد بیشتری می‌کنند. بعضی از عناصر که احساس کنترل مشتریان و در نتیجه، حس اعتماد آنها را افزایش می‌دهند، در زیر لیست شده‌اند:

*دسترسی به اطلاعات (Access to Information): سرعت و سهولت دسترسی به اطلاعات مرتبط با مشتریان در یک وب سایت، بر روی حس کنترل مشتریان در وب سایت تأثیر دارد. گزینه های مربوطه جهت آشنایی مشتریان به وب سایت مثل لغت نامه متناسب با بازدیدکنندگان، اطلاعاتی که در طول تراکنش بانکی از سوی بانک در اختیارشان قرار می‌گیرد، جواب به سوالات متداول (FAQ) و یا امکاناتی که باعث آسان تر شدن ناوبری سایت برای مشتریان کم تجربه و یا حرفه‌ای می‌شود، همگی عموماً باید در راستای مشتریان طراحی شوند[۳].

*کنترل اطلاعات شخصی (Control Personal Data): دسترسی به اطلاعات شخصی، برای بازدیدکنندگان سایت بسیار مهم است. مشتریان باید بتوانند میزان اطلاعات شخصی را که نزد بانک ها نگهداری می‌شود، تعیین کنند و زمانی که لازم بدانند، آنها را تغییر دهند. همچنین آنها باید تعیین کنند که اطلاعاتشان به صورت پیش فرض چه موقع می‌تواند در اختیار طرف های ثالث قرار گیرد. به عنوان مثال، وب سایت‌ها معمولا در طول فرآیند ثبت نام از مشتریان خود سوال می‌کنند که آیا تمایل دارند اطلاعات آنها را جهت ارسال مطالب و محصولات مورد علاقه‌شان در اختیار بانک قرار دهند یا خیر؟ مشتریان هم مختارند که آن را انتخاب نکنند، زیرا آنها معمولا احساس می‌کنند که امکان استفاده غیرمجاز از آن اطلاعات از سوی بانک‌ها وجود دارد. بنابراین، پیش بینی محتوایی که مشتریان قادرند دریافت کنند، ممکن است اعتماد آنها را در رابطه با سایت‌های بانکداری اینترنتی تحت تأثیر قرار دهد و باعث کاهش تمایل آنها نسبت به انجام امور بانکی از طریق اینترنت شود.

*آشکار سازی همه جنبه‌های روابط بین بانک و مشتری: مشتریان باید به صورت آشکار از تمامی مراحل لازم جهت تکمیل تراکنش با سایت مورد نظر اطلاع کافی داشته باشند. به علاوه، هر گونه اطلاعات مربوط به انجام تراکنش‌های بانکی مانند قابلیت اعتماد و سیاست‌های بانکی، باید قبل از تکمیل هر گونه تراکنشی، به طور صادقانه و به صورت آشکار از سوی بانک‌ها بیان شود.

*قابلیت شخصی‌سازی: وجود قابلیت شخصی‌سازی روی ظاهر سایت نیز باعث افزایش حس کنترل و اعتماد در مشتری می‌شود، زیرا مشتریان



امضای دیجیتال،از تکنیک‌های مورد استفاده برای تأیید صحت داده‌ها می‌باشد.

محتوای وب‌سایت باید متناسب باهدف بانک و نیاز مشتریان باشد و نشانگر تعصبات بی‌جا نباشد.

می‌دانند که چه می‌خواهند و کجا می‌خواهند بروند و چگونه می‌خواهند بروند. وب سایت‌ها به آنها اجازه می‌دهند تا بر اساس مشخصات فردی، تنظیمات پیش فرض را تغییر دهند، مثلا زبان، محتوا و یا هر واحد ارزیابی که متناسب با ویژگی‌های شخصی آنهاست، می تواند انتخاب شود[۳].

*بازخورد (Feed Back): اعلام تأیید از جانب سایت به مشتری پس از انجام موفق هر تراکنش بانکی، مثل ارسال ایمیل یا ارسال یک پیام به عنوان تأییدیه بعد از تکمیل هر تراکنش، ضروری است. علاوه بر آن، اعلام خطا و ارایه راه حل آن در صورت بروز مشکل نیز بسیار سودمند می‌باشد. کاهش ابهام و خطا در سمت مشتری نیز در تصمیم‌گیری مشتری بسیار کارا خواهد بود و باعث افزایش حس کنترل و اعتماد در طول عملیات بانکی از طریق سایت می‌شود.

۴-۱) تکمیل عملیات بانکی: بانک‌های اینترنتی باید به صورت آشکار مشخص کنند که چگونه تراکنش‌ها تکمیل می‌شوند و چگونه در زمان بروز مشکل، مشتریان را یاری می‌دهند. علاوه بر آن، زمانی که یک تراکنش انجام شد، یک پیغام اضافی مثل ایمیل یا فاکس می‌تواند انجام صحیح این تراکنش را تأیید کند و یک شماره به مشتری بدهد تا او بتواند برای پی‌گیری تراکنش مورد نظر خود در بانک از آن نیز استفاده کند[۲].

۵-۱) پشتیبانی از مشتریان: در بعضی از مواقع لازم است که مشتریان در مورد خصوصیات محصولات و خدمات بانکی مورد نظر خود سوال کنند، و یا اطلاعاتی در مورد حریم خصوصی و محرمانگی کسب کنند، و یا ممکن است بخواهند در مورد قابلیت محلی شدن بعضی از گزینه‌ها مطلع شوند.

مشتریان انتظار دارند که جواب این سوالات به صورت مؤثر و سریع در سایت درج شده باشد، وگرنه آنها از بانک دیگری استفاده خواهند کرد. بعضی از این گونه خدمات که باید در سایت بانکداری اینترنتی درجه شده باشند، شامل موارد زیر است:

* وجود کمک‌های مستتر که به صورت پیش فرض درون خود سایت جای دارند، مثل وجود توضیح و مقادیر پیش فرض برای هر فیلد، که به نوبه خود بعضی از ابهامات و سوالات مشتری را برطرف می‌کند.

* وجود پشتیبان اتوماتیک که به صورت آنلاین جهت کمک به کاربرانی می‌باشد که می‌خواهند گمنام بمانند، یا آنهایی که دارای مهارت کافی بر روی برنامه‌های کاربردی نیستند، و یا برای آنهایی که نسبت به زبان سایت مورد نظر دچار مشکل هستند.

* ایجاد امکان تماس با پرسنل بانک توسط ایمیل، چت و یا تلفن هم یک راه حل سریع برای رفع مشکلات مشتریان می‌باشد، آنهم در هر زمانی که آنها با سایت روبرو می شوند.

* پاسخ گویی به سوالات متداول مشتریان در قسمت FAQ یا سوالات متداول هم ضروری است.

سرعت و سهولت دسترسی به اطلاعات مرتبط با مشتریان بانک در وب‌سایت، بر روی حس کنترل مشتریان تأثیر دارد.

۲) تکنولوژی: جهت پشتیبانی از تراکنش‌های بینندگان بر روی وب‌سایت، وب سایت بانک‌ها باید از زیرساخت‌های تکنولوژی (یعنی مجموعه‌ای از سخت‌افزارها و نرم افزارها) استفاده کنند، برای اینکه بتوانند گستره وسیعی از پروسس‌ها را اجرا کنند. مواردی مثل امنیت، کارایی، مقیاس پذیری، سازگاری و قابلیت اطمینان بیشتر توسط زیرساخت‌های تکنولوژی مورد استفاده در سایت تعیین می‌شوند (همراه با تنظیمات و خصوصیات سیستم‌های مشتری). همه این موارد باید براساس خصوصیات بانک‌ها، مشخصات تراکنش‌هایی که آنها حمایت می‌کنند و نیازمندی‌ها و مشخصات مشتریان مورد انتظار باشند تا بتوانند محیط امن و مناسبی را در طول عملیات بانکی آنلاین ایجاد کنند.

۱-۲) امنیت: به طور کلی، امنیت شامل دور نگهداشتن افراد غیرمجاز از دسترسی و اجازه دادن به افراد مجاز جهت دسترسی به دارایی های با ارزش می‌باشد[۲].

سایت‌های بانکداری اینترنتی، نیازمند توسعه و استفاده از مکانیسم‌های امنیتی مناسب جهت محافظت از مشتری و بانک می‌باشند. به دلیل حرکت اطلاعات روی اینترنت، افراد غیر مجاز ممکن است به اطلاعات حساس در حین انتقال و یا بر روی سرویس‌دهنده‌های بانک دسترسی پیدا کنند، آنها را تغییر دهند و یا حذف کنند. لذا باید مکانیسمی جهت ضمانت انجام هر تراکنش بانکی که در آن داده‌های حساس مالی نیز رد و بدل می‌شوند، وجود داشته باشد. برای رسیدن به این امر مهم، از روش‌هایی

مثل رمز عبور، مکانیسم‌های رمزنگاری، امضاهای الکترونیکی و دیوارهای آتش (Firewalls) استفاده می‌شود.

در این قسمت، موارد مختلفی که برای توسعه زیرساخت‌های امنیتی سایت‌های بانکداری الکترونیکی باید مورد توجه قرار گیرند، بحث می‌شوند، مانند حریم خصوصی (Privacy)، محرمانگی (Confidentiality)، صحت اطلاعات (Integrity)، در دسترس بودن (Availability)، احراز هویت و تصدیق اصالت (Authentication)، کنترل دسترسی (Authorization)، حسابرسی (Accountability)، انکارناپذیری (Non-repudiation)، و نهایتاً نظارت و گزارشگری (Monitoring and Report).

*حریم خصوصی و محرمانگی: حریم خصوصی، یعنی صاحب اطلاعات قادر به کنترل اطلاعات خود می‌باشد؛ درحالیکه محرمانگی، به معنای پنهان بودن است، یعنی تنها گیرندگان مورد نظر یک پیام، می‌توانند آنرا بخوانند[۶]. در هر تراکنش بر روی اینترنت، اطلاعات مشتریان تنها باید توسط افراد مجاز قابل دسترس باشد، یعنی این اطلاعات باید محرمانه و خصوصی باقی بمانند[۱۳]. مشتریان لازم است مطمئن شوند که هنگام استفاده و یا ایجاد تغییر در اطلاعات، داده‌های حساس در معرض طرف‌های ثالث واقع نشوند و یا بدون کسب اجازه آنها را به طرف‌های ثالث ندهند.

رمزنگاری، پایه و اساس بیشتر روش‌های ایجاد امنیت در داده‌های موقت (مثل کوکی‌های موجود در کامپیوتر کاربران یا فایل ثبت وقایع موجود در سرویس دهنده وب) و در داده های دایمی (مثل مشخصات حساب مشتریان موجود در سرویس دهنده‌ها) می باشند.

روش‌های مختلفی برای تراکنش‌های امن در اینترنت وجود دارند که همگی بر پایه رمزنگاری می‌باشند، مثل SSL و TLS که هر دو برای حفاظت از تبادل رمز عبور و نام کاربری در حین عملیات احراز هویت و تصدیق اصالت طراحی شده‌اند[۱۴].

زیرساخت‌های حریم خصوصی، دسترسی کاربران به وب سایت‌ها را محدودتر می‌کند و در صورتی که ملاحظات مربوط به حریم خصوصی کاربران با آن سازگار نباشد، به صورت خودکار به کاربر هشدار داده می‌شود[۱۵].

*در دسترس بودن: در دسترس بودن، یعنی نگهداشتن هر سیستم به صورت فعال و در حال کار[۶]. در سایت بانکداری اینترنتی، در دسترس بودن، هم به دسترسی بموقع مشتریان به اطلاعات اشاره دارد و هم به حفظ امکان دسترسی در برابر قطع شدن سرویس مورد استفاده آنها. این امر مهم هم توسط نرم‌افزار (برنامه‌های مقیاس‌پذیر و با تحمل خطا) و هم سخت‌افزار (مثل دیسک‌ها و سرویس‌دهنده‌های مضاعف، اتصالات با پهنای باند زیاد به اینترنت و پردازنده‌های موازی) محقق می‌شود.

*صحت داده‌ها: اطلاعات دریافت شده توسط گیرنده، دقیقاً باید با اطلاعات ارسالی برابر باشند. اطلاعات موجود بر روی سرویس‌دهنده وب یا کوکی‌های موجود در کامپیوتر مشتری، نباید توسط افراد غیر مجاز تغییر کنند. تنها افراد مجاز اجازه تغییر اطلاعات را دارند که شامل نوشتن، تغییر، تغییر وضعیت، حذف و ایجاد داده جدید می‌باشد[۶]. به عنوان مثال، در مورد داده‌های داخل دستور پرداخت مانند هویت مشتری، و بانک‌ها، محتوای پرداخت، مبلغ و شماره حساب، همگی باید به صورت امن جابجا شوند. توابع درهم‌ساز (Hash Function)، کارت هوشمند، امضای دیجیتال و گواهی‌های دیجیتال از تکنیک‌های مورد استفاده در ایجاد صحت داده می‌باشند، که از الگوریتم رمزنگاری نامتقارن و الگوریتم‌های درهم‌ساز (Hash Algorithms) استفاده می‌کنند[۶].

*احراز هویت و تصدیق اصالت: افراد شرکت‌کننده در بانکداری اینترنتی (مشتری، بانک‌ها و شرکت‌های ثالث) نیاز دارند که به هویت سایر موجودیت‌های دخیل در بانکداری اینترنتی اعتماد داشته باشند. تعیین هویت مثبت، همراه با سطوحی از اطمینان، باید قبل از صدو مجوز حقوق و امتیازات مشخص به هر موجودیت قابل دسترس باشد[۷].

یک برنامه احراز هویت و تصدیق اصالت مؤثر بر پایه ریسک، باید به گونه‌ای پیاده سازی شود که مطمئن شود کنترل‌ها و روش‌های احراز هویت برای تمام محصولات و خدمات اینترنتی بانک‌ها مناسب می‌باشد و با افشای حداقل اطلاعات طرفین، عمل احراز هویت و تصدیق اصالت صورت گیرد. برای ماکزیمم کردن قابلیت همکاری با سایر

برای بازدیدکنندگان از سایت، دسترسی به اطلاعات شخصی بسیار مهم است.

در هر تراکنش بر روی اینترنت، اطلاعات مشتریان تنها باید توسط افراد مجاز قابل دسترسی باشد، یعنی اینگونه اطلاعات باید محرمانه و خصوصی بمانند.

خدمات بانکی، عمل احراز هویت و تصدیق اصالت، باید با استراتژی کلی بانک در مورد بانکداری اینترنتی و سرویس‌های مشتریان در تجارت الکترونیک سازگار باشد. روش تصدیق اصالت و احراز هویت استفاده شده در یک برنامه تحت وب خاص، باید مناسب ریسک‌های پیش‌بینی شده در آن برنامه باشد. به دلیل اینکه استانداردهای پیاده‌سازی یک سیستم بانکداری اینترنتی، با تغییر در تکنولوژی تغییر می‌کند، لذا مؤسسات مالی و بانک‌ها برای اینکه مطمئن شوند که تغییرات مناسب اعمال شده است، باید پروسه مداومی را جهت بازبینی تکنولوژی تصدیق اصالت و احراز هویت توسعه دهند.

بانک هایی که تنها از یک فاکتور جهت احراز هویت استفاده می‌کنند، در برابر ریسک‌های جدید یا تغییر یافته‌ای مانند دسترسی به اطلاعات حساس مشتریان، کدهای مخرب و سایر تکنیک‌های مخرب قرار می‌گیرند. بنابراین، ارزیابی ریسک نشاندهنده این واقعیت است که یک فاکتور جهت تصدیق اصالت و احراز هویت کفایت نمی‌کند و مؤسسات مالی و بانک‌ها باید از چند فاکتور پیاده‌سازی تصدیق اصالت و احراز هویت (مثل Pin Code و روش‌های بیومتریک به صورت همزمان)، معماری لایه لایه امنیت و سایر کنترل‌ها جهت کاهش ریسک استفاده کنند.

با رشد بانکداری اینترنتی و تجارت الکترونیکی، مؤسسات مالی باید از روش‌های قابل اعتمادی جهت ایجاد حساب برای مشتریان آنلاین استفاده کنند. در این راستا، احراز هویت مشتریان در طول ایجاد حساب ضروری می‌باشد، و در کاهش ریسک سرقت هویت، تهدیدات مربوط به برنامه حساب‌های بانکی و موافقت نامه‌ها حیاتی می‌باشد. به صورت بالقوه، زمانی که یک بانک یا مؤسسه مالی یک مشتری جدید را از طریق اینترنت یا سایر کانال‌های الکترونیکی پذیرش می‌کند، ریسک‌های پایه‌ای آن افزایش می‌یابد. یک روش تشخیص هویت مشتریان، ارایه اعتبار و هویت اثبات شده آنها از طریق طرف سوم قابل اعتماد می‌باشد. به طور مشابه، جهت ایجاد اعتبار برای یک تجارت خاص و یا توانایی یک شخص در انجام تراکنش‌هایی که بر عهده اوست، بانک‌ها مواد قانونی شرکت یا شخص،گزارش‌های اعتباری، راه حل هیأت مدیره در شناسایی مأموران و امضاکنندگان مجاز و سایر اعتبارات تجاری را مورد بازبینی قرار می‌دهند.

به هر حال، در بانکداری اینترنتی، اتکا به فرم‌های سنتی احراز هویت کاغذی اساسا کاهش می‌یابد. بنابراین، مؤسسات مالی نیازمند استفاده از روش‌های قابل اطمینان دیگری باشند[۱۸].

استفاده از گواهی‌های دیجیتال (Digital Certificate) روشی است که به صورت گسترده برای احراز هویت و تصدیق اصالت اعمال می‌شود. بانک‌ها و مشتریان می‌توانند

حریم خصوصی،یعنی صاحب اطلاعات قادر به کنترل اطلاعات خود می باشد.

به وسیله این گواهی‌ها و کلیدهای مخفی که توسط طرفین معامله استفاده می‌شوند، قانونی بودن و اعتبار هر یک از طرفین معامله را از طریق CA (Certification Authority) تصدیق کنند. SET (Secure Electronic Transaction)، یک پروتکل باز و چند طرفه است که پرداخت‌های بانکی توسط کارت را از طریق یک شبکه باز منتقل می‌کند. این پروتکل برای اینکه به طرفین معامله اجازه دهد تا هویت یکدیگر را تأیید کنند، از گواهی‌های دیجیتالی استفاده می‌کند[۷].

شناسه و رمز عبور، کارت هوشمند (حاوی کلید خصوصی) و گواهی‌های دیجیتالی (حاوی کلید عمومی) از رایج‌ترین روش‌های احراز هویت و تصدیق اصالت می‌باشند که از الگوریتم رمزنگاری نامتقارن استفاده می‌کنند[۶].

ادامه دارد

توضیح: فهرست منابع این مقاله، در پایان آخرین بخش خواهد آمد.