اولین همایش بین المللی بانکداری الکترونیک و نظام های پرداخت
تهران- ۳۰ بهمن و اول اسفند ۱۳۹۰ - مرکز همایش های برج میلاد

بانکداری الکترونیک
و نظام‌های پرداخت

شیوه های تائید اعتبار مشتریان در سیستم بانکداری الکترونیک

صادق ولی نژاد، مدرس دانشگاه پیام نور واحد کردکوی، s_valinejad@yahoo.com

چکیده

بانکداری الکترونیک نوع خاصی از بانکداری است که جهت ارائه سرویس به مشتریان خود از یک محیط الکترونیکی مانند اینترنت استفاده می کند. در این نوع بانک تمامی عملیات بانکی اعم از دریافت، واریز کردن پول، تأیید امضا، ملاحظه موجودی و دیگر عملیات بانکی به صورت الکترونیکی انجام می شود. بانکداری الکترونیک، خدمات مالی با حجم ارزشی پائین و خرد را از طریق کانالهای الکترونیکی نظیر دستگاههای خود پرداز، کارتهای اعتباری، تلفن، تلویزیون و مانند آن فراهم می سازد.

امنیت اطلاعات جزو ضروری قابلیت های یک مؤسسه مالی در جهت ارائه خدمات بانکداری اطلاعاتی است که موسسه را بر آن می دارد تا امنیت اطلاعات مشتریان را تامین کند و به آنها این اطمینان را بدهد که مسولیت هرگونه تغییر و تحول یا پردازش اطلاعات به عهده موسسه مالی بوده و همواره در قبال بروز هرگونه اشکال در سیستم های ارتباطی مشتریان با موسسه یک پاسخ مناسب و مسئولانه وجود دارد. بانک ها و موسسات مالی با توجه به گستردگی سازمان و فناوری درون سازمانی می توانند با استفاده از شبکه های کنترل کننده متعدد، امنیت اطلاعات مشتریان را که از پیچیدگی هایی خاصی برخوردار است را تامین کند. بنابراین کنترلهای مربوط به تایید یا تصدیق اعتبار مشتری نقش مهمی را در امنیت داخلی یک سازمان مالی ایفاء می کند. در مقاله حاظر، با هدف شناخت مقدماتی از بانکداری الکترونیک و مدل های رایج آن و نیز برخی موضوعات مهم مرتبط با آنها، بیان مختصری از تعاریف، اهمیت و ضرورت بانکداری الکترونیک و راههای تایئد اعتبار مشتریان در سیستم بانکداری الکترونیک پرداخته خواهد شد. در پایان مقاله نیز، موارد مذکور جمع بندی شده و در قالب

بحث و نتیجه گیری ، کاربردهای مدیریتی، و پیشنهادات مرتبط با آن، جهت پیگیری تحقیقات مشابه در آینده ارائه شده است.

کلمات کلیدی: اعتبار مشتریان، بانکداری الکترونیک، امنیت اطلاعات

۱- مقدمه

امروزه تحولات سریع و چشمگیر در زمینه فناوری اطلاعات آنچنان تأثیر شگرفی بر ماهیت سازمان، کسب وکار و اقتصاد نهاده که مدیران ارشد و سیاستگذار بدون بهره گیری از فرصت‌های بوجود آمده از این فناوری و همچنین اتخاذ جهت گیری مناسب در رویارویی با تأثیرات مبهم و گاهاً تهدیدهای این فناوری، قادر به برنامه ریزی بلندمدت و تعیین دورنمای کسب وکار سازمان نخواهند بود. سنجش اعتبار در حوزه بانکی در سطوح مختلف مطرح می‌شود. در روش‌های کارت امتیاز بر مبنای اطلاعاتی که مشتری در اختیار شرکت قرار می‌دهد، طراحی و رتبه خاصی استخراج می‌شود. در این حالت روند کار بدین صورت است که بانک، مشتری خود را به شرکت رتبه‌بندی معرفی و فرم درخواست اطلاعات را پر می‌کند. سپس این اطلاعات توسط کارشناسان، تحلیل محتوا شده و طی یک پروسه زمان‌بر مشتری حایز رتبه و امتیاز اعتباری می‌شود. با توجه به هزینه گزاف شیوه سنتی و دستی که نیازمند تاسیس شعبه در تمامی شهرها است و از سوی دیگر در دسترس بودن تکنولوژی‌های نوین و روش‌های بسیار ساده‌تر و کم‌هزینه‌تر، که کارایی بسیار بالاتری نسبت به روش‌های سنتی دارند، همچنین جلوگیری از افزایش بوروکراسی و کاغذبازی، انجام کار بدین شیوه منطقی نبود. راه حل مناسب استفاده از تکنولوژی سنجش اعتبار الکترونیکی است. در این روش مشتری به بانک مراجعه کرده و پس از تکمیل فرم درخواست تسهیلات، کارمند بانک می‌تواند با وارد کردن اطلاعات مشتری و دادن کد اختصاصی، گزارش اعتباری مشتری را دریافت کند (جلیلی، ۱۳۸۸).

در این مقاله روشهای تأئید اعتبار مشتری مورد بحث قرار خواهد گرفت. ابتدا مروری کوتاه بر مفاهیمی همچون بانکداری الکترونیک و امنیت اطلاعات دربانکداری الکترونیک خواهد داشت. در ادامه به چند روش برای تائیید اعتبار مشتری اشاره خواهد شد. در پایان پسشنهاد شده است که ارتقای سطح امنیت سیستمهای موجود و ترویج خدمات از طریق گسترش سایتهای بانکی می تواند زمینه ساز رشد بانکداری الکترونیکی را فراهم سازد.

۲- مفهوم بانکداری الکترونیک

بانکداری الکترونیک نوع خاصی از بانکداری است که جهت ارائه سرویس به مشتریان خود از یک محیط الکترونیکی مانند اینترنت استفاده می کند. در این نوع بانک تمامی عملیات بانکی اعم از دریافت، واریز کردن پول، تأیید امضا، ملاحظه موجودی و دیگر عملیات بانکی به صورت الکترونیکی انجام می شود.بانکداری الکترونیک، خدمات مالی با حجم ارزشی پائین و خرد را از طریق کانالهای الکترونیکی نظیر دستگاههای خود پرداز[i]، کارتهای اعتباری، تلفن، تلویزیون و مانند آن فراهم می سازد(Pennathar, 2001). این نظام از این جهت بانکداری مجازی اطلاق می شود که ارائه خدمات بانکی را با ابزارهای جدید، فناوری های مختلف و متفاوت از بانکداری سنتی ارائه می دهد(Liao et al., 1999). بانکداری الکترونیک به دلیل نیازهای بازار و تغییرات سریع محیطی، بانکها و مشتریان آنها خواستار دستیابی به رویکردهای مختلف الکترونیک است. جدول شماره ۱ زاویه تحلیلی گذار بانکداری سنتی به بانکداری الکترونیک را از پنج منظر نشان می دهد.

به طور کلی بانکداری الکترونیکی عبارت است از فراهم آوردن امکاناتی برای کارکنان در جهت افزایش سرعت و کارایی آنها در ارائه خدمات بانکی در محل شعبه و همچنین فرآیند های بین شعبه ای و بین بانکی در سراسر دنیا و ارائه امکانات سخت افزاری و نرم افزاری به مشتریان که با استفاده از آنها بتوانند بدون نیاز به حضور فیزیکی در بانک، در هر ساعت از شبانه روز (۲۴ ساعته) از طریق کانال های ارتباطی ایمن و با اطمینان عملیات بانکی دلخواه خود را انجام دهند. به عبارت دیگر بانکداری الکترونیکی استفاده از فناوری های پیشرفته نرم افزاری و سخت افزاری مبتنی بر شبکه و مخابرات برای تبادل منابع و اطلاعات مالی به صورت الکترونیکی است که می تواند باعث حذف نیاز به حضور فیزیکی مشتری در شعبه بانک ها شود.

جدول شماره ۱- ویژگی های بانکداری سنتی و بانکداری الکترونیک

منظر	بانکداری سنتی	بانکداری الکترونیک
هدف	ارائه خدمات استاندارد به ب مشتریان	ارضای نیازهای مشتریان
محور توجه	محصولات/خدمات	مشتریان
اطلاعات درباره مشتریان	کمی	کمی و کیفی
فرایند	مشتریان در انتهای زنجیره تأمین قرار دارند	مشتریان در ابتدای زنجیره ارزش قرار دارند
روشهای بازاریابی	تجزیه و تحلیل گروهی	استنباط علائق

Source:Fridgen,et al,2001

سیستم‌های بانکداری الکترونیکی به همه این امکان را می‌دهد که سریع و آسان به کارهای بانکی خود مانند دریافت موجودی حساب، انتقال پول میان حساب‌های گوناگون یک مشتری، انتقال پول از حساب یک مشتری به حساب مشتری دیگر و دریافت صورت حساب بانکی در یک دوره ویژه دسترسی داشته باشند. برخی از بانک‌ها خدماتی مانند انتقال سهام و ارسال فایل‌های پرداخت از یک حساب مشخص به حساب افراد گوناگون (مانند پرداخت حقوق) را نیز انجام می‌دهند. با گسترش فناوری، انواع سیستم‌های بانکداری الکترونیکی نیز ایجاد شده است که هر یک از آنها ابعادی تازه را در زمینه تبادل اطلاعات میان کاربر و بانک ارایه می‌کنند. ATM نخستین سیستم شناخته شده‌ای است که برای آسانی دسترسی کاربران به فعالیت‌های بانکی خود معرفی گردید. به‌کمک یک رابط گرافیکی کاربر (UGI2)، کاربر می‌تواند برخی از این کارها را اجرا کند و این عملیات به سیستم کامپیوتر مرکزی بانک منتقل می‌گردد. گام بعدی، معرفی بانکداری تلفنی بود. کاربران با تلفن از خانه به سیستم کامپیوتری بانک متصل شده، با کلیدهای تلفن کار بانکی خود را انجام می‌دادند. اینترنت نیز یک جایگزین تازه برای سیستم بانک تلفنی پیشنهاد کرده است. مردم با یک رابط کاربرپسند و پیچیده‌تر، یک مرورگر یا برنامه کاربردی استاندارد، می‌توانند در اینترنت به سیستم کامپیوتری بانک راه یابند. ابزارهای الکترونیکی همواره در حال کوچک شدن هستند، در حالی‌که کارایی آنها افزایش می‌یابد. هم‌اکنون، تلفن همراه نیز امکان اجرای سیستم بانکداری الکترونیکی را فراهم آورده است.

۳- مدل های رایج بانکداری الکترونیک

۳-۱- بانکداری اینترنتی

بانکداری اینترنتی نوع خاصی از بانکداری الکترونیک است که از اینترنت به عنوان کانال توزیع استفاده می کند. یک بانک اینترنتی در واقع وسیله ای است که فقط رو ی اینترنت یا سابر شبکه های توزیع موجود است و دارای هیچگونه شعبه فیزیکی نیست. این چارچوب کاری باعث می شود که بانکی داشته باشیم که نیازی به امور کاغذی ندارد، محدود به مناطق جغرافیایی خاصی نیست و هیچ گاه به روی مشتریان بسته نمی شود و می تواند به صورت ۲۴ ساعته به مشتریان سرویس بدهد. بانکداری اینترنتی زیرمجموعه بانکداری تحت وب است. در این رویکرد، تنها رسیدگی به امور مالی شخصی مشتریان از طریق صفحات وب بانکی انجام نمی گیرد بلکه تمامی خدمات مالی در سطح خرد و کلان با استفاده از کانال های ارتباطی انجام می پذیرد(Crede, 1999).

۳-۲- بانکداری مبتنی بر شعبه های الکترونیکی

شعبه الکترونیک به این صورت است که بانکهای معمولی و مرسوم، خدمات بانکداری الکترونیک نیز به کاربران خود ارائه می دهند. بانکداری الکترونیکی به عنوان ابزارها، تکنیک ها و راه حل های خودکار سازی فرآیند ارایه مستقیم محصول ها و خدمت های مختلف و متنوع در بانکداری سنتی و جدید به مشتریان از طریق کانال های ارتباطی دو سویه، تعریف می شود. بانکداری الکترونیکی شامل سیستم هایی است که مشتریان، افراد مختلف یا بنگاه های تجاری و غیر تجاری را قادر می سازد تا به حساب ها و تراکنش های مالی شرکت خود دسترسی داشته و یا اطلاعاتی در زمینه محصولات و خدمات از طریق شبکه های خصوصی و عمومی اطلاع رسانی همچون اینترنت به دست آورند.

۴- امنیت تبادل داده های شخصی در بستر الکترونیک

فناوری اطلاعات همانند سایر فناوری ها دو رو دارد: فرصت ها و تهدیدها. اگر به همان اندازه که به توسعه و فراگیری آن توجه می کنیم، به امنیت آن توجه نکنیم، می تواند به یک تهدید و مصیبت بزرگ تبدیل شود(محمودزاده، ابراهیم(۱۳۸۵). یکی از مواردی که تاثیر منفی زیادی در عدم رغبت مدیران و کاربران برای توسعه تجارت الکترونیک می گذارد، عدم بستر سازی مناسب در زمینه امنیت تبادلات داده های شخصی و محرمانه مانند اطلاعات پرداخت الکترونیک شامل شماره های حساب و رمز کارت و ... می باشد(اکبری ،۱۳۸۵). امنیت اطلاعات جزو ضروری قابلیت های یک مؤسسه مالی در جهت ارائه خدمات بانکداری اطلاعاتی است که موسسه را بر آن می دارد تا امنیت اطلاعات مشتریان را تامین کند و به آنها این اطمینان را بدهد که مسولیت هرگونه تغییر و تحول یا پردازش اطلاعات به عهده موسسه مالی بوده و همواره در قبال بروز هرگونه اشکال در سیستم های ارتباطی مشتریان با موسسه یک پاسخ مناسب و مسئولانه وجود دارد. بانک ها و موسسات مالی با توجه به گستردگی سازمان و فناوری درون سازمانی می توانند با استفاده از شبکه های کنترل کننده متعدد، امنیت اطلاعات مشتریان را که از پیچیدگی خاص خودش برخوردار است تامین کند(رحیمی مقدم،۱۳۸۷). امنیت به بیان ساده محافظت از منفعت می باشد. مردم می خواهند از پولهای خودشان و بانکها از کیفیت ارائه خدماتشان می خواهند محافظت کنند. نقش دولت محافظت از درستی فرایند و محافظت از کل سیستم می باشد. با پول الکترونیک دولت باید مجموعه را از ریسک سیستمی محافظت نماید، همانطور که تا به حال در

مورد پول کاغذی انجام داده است، این یک نقش جدی است که نمی توان به موسسات کوچک واگذار نمود(Chaum,1992).

۵- تایید اعتبار مشتریان

در بانکداری الکترونیک، مشتری، کاربرمستقیم فناوری موسسه مالی است. مشتریان باید وارد سیستم موسسه شده و ازآن استفاده کنند. بر همین اساس موسسه مالی باید دسترسی مشتریان به سیستم را تحت کنترل و نظارت قرار داده و موارد مربوط به مسئولیت های امنیتی آنان را به آنان آموزش دهند. کنترل های مربوط به تائید اعتبار مشتری نقش مهمی در امنیت داخلی یک سازمان ایفا می کند.

نظام سنجش اعتبار سیستم بزرگی است که در برگیرنده زیرمجموعه‌هایی همچون بازار اعتبار، محیط شرکت اعتبار سنجی، منابع اطلاعاتی و... است که کل این مجموعه ها در چارچوب نظام حقوقی و قانونی قرار دارد. اعتبارسنجی به دانش فنی ویژه و منحصر به فردی نیاز دارد. پنج مؤسسه بزرگ اعتبارسنجی بین المللی: Experian , TransUnion, Equifax, Schufa, Credit info این کار را در سطح بین المللی انجام می دهند.

در ایران نیز شرکت مشاوره و رتبه‌بندی اعتباری ایران از سال ۱۳۸۵ با همت معاون بانک، بیمه و شرکت‌های دولتی وزارت امور اقتصادی و دارایی و مشارکت کلیه بانک‌های کشور و با کمک شرکت Credit info تاسیس شد. این شرکت در حال حاضر کلیه زیرساخت‌های مورد نیاز را با بهره‌گیری از توانمندی داخلی و دانش فنی موسسات بین‌المللی رافراهم کرده و اجرای آزمایشی و پایلوت آن از مهر ۱۳۸۷و اجرای نهایی آن از آذر ۱۳۸۷ در بانک‌های کشور آغاز شده است (جلیلی، ۱۳۸۷). عملیاتی شدن سیستم جامع سنجش اعتبار در نظام بانکی کشور، به عنوان یکی از ابعاد بانکداری الکترونیکی در حوزه اعتباری محسوب می‌شود(جلیلی، ۱۳۸۸).

۵-۱- تایید اعتبار مشتریان جدید

بازبینی یا وارسی هویت مشتریان، خصوصا مشتریان جدید، جز لاینفک و ضروری تمام سرویسهای مالی است . هر موسسه مالی باید اقدام بهارائه و اجرای یک برنامه شناسایی مشتری یا CIP کندبه طوری که با موقعیت، گستردگی و نوع فعالیت کاری موسسه مطابقت داشته باشد. برنامه شناسایی یا تعیین هویت مشتری باید مکتوب و در برنامه یا مقررات ضد پولشویی موسسه مالی گنجانده شده، سپس به تایید هیأت مدیره موسسه

برسد. هنگام بکارگیری رو شهای وارسی هویت مشتری باید ریسکهای موجود را نیز شناسایی و ارزیابی کـرد. این رو شها عموما شامل مشتریانی می شود که حسا بهای جدید افتتاح می کنند. رو شـهای برنامـه شناسـایی مشتری باید مشخص کند که بانک چگونه با استفاده از رو شهای مستند، غیر مستند و یا ترکیبی از هر دو می تواند هویت واقعی مشتری را احرازکند.

روشهای مذکور مراحل و نحوه افتتاح حساب در موسسه چه به صورت حضوری و یا غیرحضوری را بـه عنـوان قسمتی از خدمات بانکداری الکترونیکی شامل می شود. یک موسسه مالی به عنوان قسمتی از رو شـهای غیـر مستند وارسی هویت مشتری می تواند از همکاری اشخاص ثالث برای تعیین هویـت و تاییـد اعتبـار مشـتریان جدید استفاده کند. در این گونه موارد، مسئولیت اعتماد به رو شهای مورد استفاده اشخاص ثالث در شناسایی و تایید هویت مشتری متوجه موسسه مالی است. تکمیل فر مهای مربوط به افتتاح حسا بهای جدید بـه صـورت آنلاین، مشکلات مربوط به بررسی هویت مشتریان را افزایش می دهـد. از ایـن رو تعـدادی از موسسـات مـالی همچنان ترجیح می دهند تا مشتریان به دفتر یا شعبه موسسه مراجعه و مراحل افتتاح حساب را حضوری انجام دهند. موسسه هایی که مراحل افتتاح حساب در آنها به صورت کاملا الکترونیکی انجام می شود و از اطلاعـات پایگاه داده های شخص ثالث استفاده می کنند، باید نسبت به موارد ذیل آگاهی و اطمینان حاصل کنند.

۱- وارسی مثبت: به معنای آن است که اطلاعات متقاضی افتتاح حساب با اطلاعات موجود در منابع پایگـاه داد ه های شخص ثالث همانند است.

۲- وارسی منطقی: به مفهوم اطمینان از مطابقت اطلاعات متقاضی با اطلاعات موجود است.

۳-وارسی منفی: بدان معناست که اطلاعات متقاضی مربوط به شخصـی اسـت کـه سـوء پیشـینه جعـل یـا کلاهبرداری دارد(رحیمی،۱۳۸۷).

۵-۲- تایید اعتبار مشتریان فعلی

موسسات مالی باید علاوه بر شناسایی هویت مشتریان، نسبت به تصدیق هویت یا تایید اعتبار آنان بـه هنگـام برقراری ارتباط بر خط(آنلاین) با شبکه و دسترسی به اطلاعات موسسه مالی، اقـدام کننـد. روشـی را کـه یـک موسسه مالی برای تایید اعتبار مشتریان به کار می برد باید متناسب با نوع خدماتی باشد که از طریق سیسـتم بانکداری الکترونیکی به مشتریان ارائه می شود، مضافا این که با احتساب ریسک های مربوطه، به لحاظ تجاری نیز معقول و منطقی باشد. تشخیص این موضوع که روش مورد استفاده تا چه حد از نظر تجاری توجیه پذیر می

باشد، به ارزیابی موقعیت و شرایط بستگی دارد. موسسات مالی باید هزینه رو شهای وارسی هویت و تایید اعتبار مشتریانشان را با در نظر گرفتن فناوری و فرآیند پردازش، میزان حساسیت نقل و انتقالات مالی، اطلاعات مربوط به مشتریان و موسسه و سطح امنیت و حفاظت لازم مورد ارزیابی قرار دهند. آن چه که به کارگیری یک روش را به لحاظ تجاری معقول و منطقی می سازد ممکن است با گذشت زمان و تحول فناوری و استانداردهای مربوطه، تغییر کند.

روش های تایید اعتبار مشتری شامل تایید حداقل یک مورد از عوامل ذیل می شود:

۱- عاملی که در اختیار مشتری قرار گرفته است مثل کارت خود پرداز یاکارت هوشمند۲-عاملی که فقط مشتری باید از آن اگاه باشد مثل یا PIN یاکلمه عبور ۳-عاملی که فقط مشتری باید از آن آگاه باشد مثل عواملی نظیر اثر انگشت یا اسکن چشم که از ویژگی های زیستی خاص هر مشتری می باشد. رو شهای مبتنی بر تایید بیش از یک عامل برای تایید اعتبار مشتری، معمولا دشوارتر از روش های تک عاملی هستند و از این رو فرآیند موثق تر و مطمئن تری را ایجاب می کنند. به عنوان مثال استفاده از شناسه مشتری به همراه کلمه عبور، یک روش تک عاملی محسوب می شود چرا که مشتری از هر دوی این عوامل که جزو گروه اول می باشند آگاهی کامل دارد. اما یکی از متداو ل ترین رو شهای دو عاملی در نقل و انتقالات مشتری از طریق دستگا ههای خودپرداز به کار گرفته می شود بطوریکه مشتری و کلمه عبور ارائه م یشود .بعضی از کارشناسان امنیتی استفاده ازکلمه عبور را به دلایل مختلف مورد انتقاد قرار می دهند. از جمله آن که نرم افزارهای رمزشکن و پرداز ههای ورود به سیستم می توانند بدون توجه به رمزگذاری صورت گرفته، کلمه عبور را حدس زده و از آن عبور کنند. علت مقبولیت این نوع تایید برای ورود به سیستم آسان بودن استفاده از آن توسط عامه مردم و نیز سازش پذیری این روش با زیرساختهای رایانه ای موجود است.

آن دسته از موسسات مالی که به مشتریان خود اجازه می دهند تا ازکلمات یا رمزهای عبور کوتاه که براحتی قابل تشخیص هستند استفاده کنند مثل اطلاعات شخصی مشتری اعم از شماره شناسنامه یا گواهینامه و یا تاریخ تولد که عموم مشتریان از آنها برای ساخت کلمات عبور خود استفاده کنند، ممکن است در معرض تهدیدهای امنیتی بیشتر از سوی هکرها و سوءاستفاده کنندگان درون سازمانی قرار گیرند. اتخاذ تدابیر امنیتی قوی تر درساختار و بکارگیری کلمات عبور به کاهش چنین ریسکهایی کمک می کند. روش دیگر کاهش ریسکهای ناشی از حملات پرداز ه ای به کارگیری شناسه کاربر بدون یک ترتیب خاص است به طوری که دارای یک ساختار مشخص نبوده و یا در ساخت آن از اطلاعات متداول و قابل دسترسی استفاده نشده باشد. امنیت کلمات عبور از سه جنبه قابل بررسی است که عبارتند از:

۵-۲-۱- اختفای کلمه عبور

امنیت سیستمهایی که ورود به آنها فقط براساس کلمه عبور تعریف شده است به اختفا یا پنها ن سازی کلمه عبور بستگی دارد. چنانچه شخص دیگری کلمه عبور را بدست آورد می تواند وارد سیستم شده و همانند کاربر اصلی نقل و انتقالاتی را انجام دهد. رفتار مشتریان در شبکه و رو شهای دستیابی به کلمات عبور، امنیت کلمات عبور را به مخاطره می اندازد. مهاجمان رایان های می توانند نقاط ضعف شبکه را شناسایی کرده و به سیستم های سازمانی متصل به اینترنت (یا رایانه های خدمات رسان) واردشده و به فایلهای مربوط به کلمات عبور دسترسی یابند. به علت این گونه آسیب پذیر ی ها، کلمات عبور و فایلهای مربوط به آنها باید هنگام ذخیره سازی یا انتقال به شبکه های باز مثل اینترنت حتما به صورت رمز شده درآید. سیستم باید طوری طراحی شده باشد که به هیچ کاربری اعم از سیستمی یا اداری اجازه ندهد تا کلمات عبور را به صورت غیر رمز مشاهده کرده یا از آن چاپ بگیرد. علاوه بر این، پرسنل امنیتی باید مطمئن باشند که فایلهای مربوط به کلمات عبور کاملا حفاظت شده هستند و تحت کنترل و نظارت دقیق قرار دارند زیرا در صورت سرقت، مهاجمان رایانه ای می توانند فایل کلمات عبور رمزسازی شده را از حالت رمز خارج کنند. موسسات مالی باید اهمیت محرمانه بودن کلمه عبور را به مشتریان یادآور شده و بر حفظ آن تاکید کنند. همچنین خروج از سیستم هنگام عدم نیاز به آن، خصوصا سیستم هایی که از طریق شبکه قابلیت دسترسی به سیستمهای بانکداری الکترونیکی موسسات مالی را دارند مثل سیستم های موجود در کافی نت ها، کتابخانه ها و لابی هتل ها، ریسک استفاده غیر مجاز از کلمات عبور راکاهش می دهد.

۵-۲-۲- تعداد و ترکیب کارآکترهای کلمه عبور

تعداد و ترکیب مناسب کارآکترهای کلمه عبور به ارزش یا میزان حساسیت اطلاعاتی بستگی دارد که بوسیله کلمه عبور حفاظت می شود.کدهای شناسایی متداول مثل اسامی اشخاص، شماره شناسنامه یا گواهینامه و همین طور کلمات انتخاب شده از یک فرهنگ لغت را نباید به عنوان کلمه عبور استفاده کرد. ترکیب استاندارد کلمه عبور که معمولا شامل اعداد و نمادها به همراه حروف بزرگ و کوچک الفبا به صورت نامرتب می‌باشد می تواند یک وسیله دفاعی قو ی تر را در مقابل برنامه های رمزشکن فراهم آورد. سیستمهایی که به شبکه های باز مثل اینترنت متصل می شوند دراختیار گروه بیشتری از اشخاص قرار دارند که ممکن است سعی در به خطر انداختن سیستم داشته باشند. مهاجمان رایانه ای می توانند با استفاده از برنامه هایی که به صورت اتوماتیک

میلیو نها ترکیب از کلمات عبور را ایجاد می کنند، کلمه عبور یک مشتری را کشف کنند یا اصطلاحا به یک حمله بی رحمانه دست بزنند. یک موسسه مالی می تواند با ارائه راهنمایی وآموز شهای لازم به پرسنل و مشتریان در چگونگی انتخاب کلمات عبورمناسب و سنجیده و همین طور حفاظت لازم از فایل کلمات عبور، ازخطرات مربوط به این قسمت بکاهد.

۵-۲-۳- کنترل های اجرایی کلمه عبور

هنگام بررسی و ارزیابی سیستمهای بانکداری الکترونیکی که فقط از کلمه عبور استفاده می کنند، باید قابلیتهای سیستم را در خصوص کنترل و تایید مشتریان در نظر گرفت. این نوع قابلیتهای سیستمی که باید در راستای سیاستهای امنیتی موسسه تعریف شده باشند عبارتند از: الزامات در نظر گرفته شده برای تعداد و ترکیب کارآکترهای کلمات عبور، قفل کردن سیستم در صورت ورود نادرست، مهلت انقضای کلمات عبور، به کارگیری برنامه تکرار کلمه عبور برای ورود به سیستم، الزامات رمزسازی فایلها به همراه انواع رو شهای نظارتی و گزارشگیری از خطاهای سیستم به هنگام بهره برداری. هر موسسه مالی با توجه به ماهیت اطلاعاتی در دسترس و نقل و انتقالات مالی، باید میزان ریسک توام با روشهای کنترل و تایید مشتریان را مورد بررسی و ارزیابی قرار دهد .موسساتی که فقط بر اساس کلمه عبور، خدمات بانکداری الکترونیکی را در اختیار کاربران یا مشتریان خود قرار می دهند باید از استانداردهای قوی اجرایی و نظارتی استفاده کنند.

۵-۳- کنترل های اداری در بانکداری الکترونیکی

فعالیتهای بانکداری ا لکترونیکی همانند سایر فرآیندهای عملیات بانکی ریسک پذیر هستند. اما روش های کنترل اداری و نظارت بر ریسکهای وارده بر بخش بانکداری الکترونیکی متفاوت با سایر بخشهاست، به علت آنکه خدمات بانکداری الکترونیکی تا حد زیادی به سیستمهای مکانیزه وابسته بوده وامکان دسترسی مستقیم(بدون حضور یا واسطه کارکنان موسسه مالی) مشتری به شبکه رایانه موسسه امکا نپذیر می باشد . برخی رو شها و کنترلهای لازم که به دسترسی پذیری و درجه اطمینان داده های سیستمهای بانکداری الکترونیکی کمک می کند به شرح ذیل میباشد:

۵-۳-۱- تفکیک وظایف کارکنان

پشتیبانی خدمات بانکداری الکترونیک تا حد زیادی به پرسنل عملیات سرویس دهی که شامل کارکنان بخشهای دفترداری و نگهداری حسا بها، خدمات مشتریان، عملیات اجرایی شبکه و همین طور کارکنان بخش امنیت اطلاعات می شود، وابسته است. به عبارت دیگر هیچ یک از پرسنل به تنهایی قادر به پشتیبانی فرآیند نقل و انتقالات مالی از ابتدا تا به انتها نمی باشند. مدیریت موسسه باید در بخشهایی که وظایف پرسنل با یکدیگر تداخل داشته، شناسایی کرده و با به حداقل رساندن همپوشانی یا تداخل وظایف، از سوء استفاده یا کلاهبردار ی های احتمالی کاربران درون سازمانی جلوگیری کند .به عنوان مثال، کارکنان عملیات اجرایی شبکه که مسئول پیکربندی سرورها و دیوار ههای آتش هستند نباید جزء افرادی باشند که مسئولیت مطابقت بخشهای دسترسی به شبکه را با تدابیر و سیاستهای امنیتی سازمان به عهده دارند. همچنین کارکنان بخش خدمات مشتریان که به اطلاعات محرمانه حسا بهای مشتریان دسترسی دارند، نباید مسئولیتی در بخش کنترل روزانه نقل و انتقالات مالی الکترونیکی موسسه داشته باشند.

۵-۳-۲- کنترل های دوگانه

بعضی از نقل و انتقالات مالی مشتریان که از نظر موسسه از حساسیت خاص برخوردار است باید قبل از تایید نهایی توسط حداقل دو نفر از پرسنل مربوطه کنترل شود. نقل و انتقال الکترونیکی وجوه کلان و یا دسترسی به کلیدهای رمز از جمله مواردی هستند که حتما باید تحت کنترل دوگانه صورت گیرد.

۵-۳-۳- مطابقت های لازم

سیستمهای بانکداری الکترونیکی باید با ایجاد کنتر لهای ضد کلاهبرداری و انجام عملیات شناسایی اقدامات متقلبانه، امکان بررسی فوری اقدامات مشکوک و ارائه گزار شهای لازم را فراهم آورند .برخی از نگرانی های موجود در این زمینه عبارتند از: اطلاعات جعلی یا نادرست متقاضی، سپرده های جاری کلان در حسابهای جدید الکترونیکی، نقل و انتقال وجوه با حجم زیاد یا غیر معمول، چند حساب جدید با اطلاعات یکسان و مشابه که از یک آدرس اینترنتی نشأت گرفته باشد و همین طور عملیات غیر عادی در حسا بهایی که دارای آدرس اینترنتی در خارج ازکشور هستند.

۵-۴- وب سایت با اسامی مشابه

موسسات مالی باید در انتخاب اسم وب سایت دقت کافی را به عمل آورند به طوری که از تشابه اسمی با سایر وب سایتها به علت اشتباهات و سردرگمی های احتمالی جلوگیری به عمل آورند. این موسسات باید بهصورت دور ه ای اینترنت را مورد جستجو قرار داده و وب سایتهایی را که اسامی مشابه دارند شناسایی کنند. مخصوصا وب سایتهایی که ظاهرآنها شبیه به موسسه مالی است باید مورد تحقیق و بررسی قرار گیرد و در صورت مشکوک بودن در اسرع وقت به مقامات قانونی و قضایی ذیربط معرفی شوند.

۵-۵- بازبینی ها

سرعت عملیات بانکداری الکترونیکی فرصت زیادی را برای مشتریان فراهم نمی آورد تا چنانچه در خصوص عملیات نقل و انتقال مالی مورد نظرشان سوالاتی دارند، رفع اشکال کنند. از این رو موسسات مالی باید تدابیر و روش هایی را برگزینند تا احتمال خطا یا سردرگمی مشتریان را به حداقل رسانده، از انجام نقل و انتقالات مالی ناخواسته جلوگیری به عمل آورند. به همین منظور، گنجاندن توضیحات کافی در قرار داد فی مابین بانک و مشتری که حقوق و مسئولیتهای طرفین را به وضوح مشخص کند، امری ضروری است. همچنین فراهم آوردن منوی راهنما و دستورالعمل های لازم که گویای نحوه انجام عملیات مالی از طریق شبکه بانکداری الکترونیکی باشد و تاییدهای لازم را برای انجام فرایند نقل و انتقال مالی از مشتری دریافت کند، کمک موثری برای این منظور خواهد بود.

استفاده از سیستم بازبینی خطا در فرم های آنلاین که از طریق شبکه در اختیار مشتریان قرار می گیرد. می تواند از بروز اشتباهات متداول جلوگیری کند. وجود گزینه های دو سویه یا تعاملی برای تاییدعملیات مالی نیز مشتری را بر آن می دارد تا دستوراتی را که به سیستم داده است، قبل از انجام عملیات نقل و انتقال مالی، بازبینی و تایید کند. به عنوان مثال، چنانچه مشتری برای پرداخت صورت حساب، مبلغ وتاریخ را به سیستم وارد و ذینفع صورت حساب را نیز مشخص کرده است، سیستم باید قبل از انجام عملیات مالی از مشتری در خواست کند که کلیه دستوراتش را بازبینی کرده و سپس صحت دستورات را با کلیک تایید کند.

۵-۶- نظارت بر تداوم ارائه خدمات

در دسترس بودن شبانه روزی خدمات بانکداری الکترونیکی بدون هرگونه قطع ارتباط سیستمی حداقل انتظار مشتریان موسسه مالی می باشد. چنانچه خدمات بانکداری الکترونیکی به صورت متنوع نیز ارائه شود بر روابط بین مشتریان و موسسه مالی تاثیر بسزایی خواهد گذاشت. با توجه به همین تاثیر گذاری، موسسات مالی باید

قطع احتمالی ارتباط سیستمی و سرویس های ارائه شده را مورد بررسی و تجزیه و تحلیل قرار داده و نسبت به کاهش این گونه موارد و همین طور به حداقل رساندن زمان بازسازی فایل های آسیب دیده اقدام کنند. همچنین به روزرسانی و توسعه سیستم های درگیر در بانکداری الکترونیکی و ارزیابی دوره ای توانایی این سیستم ها در ارائه خدمات مورد انتظار مشتریان باید از سوی مدیران موسسه مالی در اولویت قرار گیرد. ممکن است برخی بانک ها و موسسات مالی با توجه به حجم فعالیت ها، تعداد مشتریان و میزان دسترسی مشتریان به خدمات بانکی از طریق سایر روش هایی که در شعب بانک ارائه می شود، خدمات بانکداری الکترونیکی را به عنوان یک اولویت یا نیاز درجه اول ندانند. اما واقعیت آن است که ارزیابی دوره ای سیاستگذاری و برنامه های مدیران موسسه مالی در ارائه خدمات و داشتن یک استنباط درست از نیازهای مشتریان و تعامل آنان با موسسه، پشتوانه ای منطقی و محکم برای رشد و توسعه خدمات بانکداری الکترونیکی و تداوم آن خواهد بود.

۶- نتاج و یافته ها

همانگونه که در متن مقاله به آن اشاره شده است. با گسترش فناوری، انواع سیستم‌های بانکداری الکترونیکی نیز ایجاد شده است که هر یک از آنها ابعادی تازه را در زمینه تبادل اطلاعات میان کاربر و بانک ارایه می‌کنند. سیستم‌های بانکداری الکترونیکی همچنین به همه این امکان را می‌دهد که سریع و آسان به کارهای بانکی خود مانند دریافت موجودی حساب، انتقال پول میان حساب‌های گوناگون یک مشتری، انتقال پول از حساب یک مشتری به حساب مشتری دیگر و دریافت صورت حساب بانکی در یک دوره ویژه دسترسی داشته باشند. برخی از بانک‌ها خدماتی مانند انتقال سهام و ارسال فایل‌های پرداخت از یک حساب مشخص به حساب افراد گوناگون (مانند پرداخت حقوق) را نیز انجام می‌دهند. یکی از موضوعاتی که نقش بسار مهمی در سیستم بانکداری الکترونیک ایفا می کند، تائید اعتبار مشتریان است. در بانکداری الکترونیک، مشتری، کاربرمستقیم فناوری موسسه مالی است. مشتریان باید وارد سیستم موسسه شده و ازآن استفاده کنند. بر همین اساس موسسه مالی باید دسترسی مشتریان به سیستم را تحت کنترل و نظارت قرار داده و موارد مربوط به مسئولیت های امنیتی آنان را به آنان آموزش دهند. کنترل های مربوط به تائید اعتبار مشتری نقش مهمی در امنیت داخلی یک سازمان ایفا می کند. بنابر این روشی که یک موسسه مالی برای تائید اعتبار مشتریان به کار می برد باید متناسب با نوع خدماتی باشد که از طریق سیستم بانکداری الکترونیک به مشتریان ارائه می شود. علاوه بر اینکه با ریسک های مربوطه، به لحاظ تجاری نیز معقول و منطقی باشد.

۷- جمع بندی

۷-۱ بحث و نتیجه گیری

همانگونه که بیان شد هدف از نگارش مقاله حاضر، تائید اعتبارمشتریان در سیستم بانکداری الکترونیک بوده است.. لذا در مقاله حاضر بمنظور دستیابی به اهداف مطرح شده ضمن بیان مختصر از ادبیات موجود به بررسی مفاهیم مرتبط با بانکداری الکترونیک پرداخته شد و در ادامه تعاریفی متعدد و نمونه هایی رایج ازبانکداری الکترونیک را بیان نمودیم و بعد از آن به عنوان یک نوآوری به بسط و توضیح چگونگی تائید اعتبار مشتریان در سیستم بانکداری الکترونیک و در ادامه هر یک از این اجزاء به تفصیل مورد نقد و بررسی قرار گرفت. در بخش بعد کنترل های اداری در بانکداری الکترونیک و برخی روشها و کنترلهای لازم که به دسترسی پذیری و درجه اطمینان داده های سیستمهای بانکداری الکترونیکی کمک می کند، پرداخته شده است.

۷-۲- پیشنهادات و کاربرد های مدیریتی

پیاده سازی بانکداری الکترونیک در کشورهایی مانند کشور ما مستلزم وجود کلیه زمینه های فرهنگی، اقتصادی، سیاسی، تکنولوزیک و حتی آموزش به عنوان می باشد. ضرورتاً کلیه خدمات نیز باید متناسب با ساختار سنتی و مدرن جامعه قانونی شوند تا سرمایه گذاری بر روی این امکاناترا توجیه نماید وامکان موفقیت را افزایش دهد.همانگونه که فناوری پیشرفت می کند، بیشتر کارهای رئزانه نیز به سوی بر خط شدن پیش می رود.بانکداری الکترونیک یکی از مهمترین نمونه های این روند است. بحث های ارائه شده می تواند در تجارت الکترونیکی، دولت الکترونیکی و دیگر خدمات الکترونیکی هم کاربرد داشته باشد. نخستین موضوع مهم امنیت، ایجاد یک کانال امن است. داده‌ها یکپارچه و با اطمینان میان کاربر و بانک تبادل می‌شود. موضوع مهم امنیت هم احراز هویت کاربر در هنگام ارتباط وی با بانک است. رمزهای ثابت همچنان به‌گستردگی به‌کار خواهد رفت، زیرا کاربردی ساده دارد، اما از نظر امنیتی آسیب پذیر است. موسساتی که فقط بر اساس کلمه عبور، خدمات بانکداری الکترونیکی را در اختیار کاربران یا مشتریان خود قرار می دهند باید از استانداردهای قوی اجرایی و نظارتی استفاده کنند. حتی بهترین راه‌حل هم بستگی به این دارد که سیستم چه‌اندازه قابل اطمینان باشد. کاربر مسوولیت امنیت دستگاه خویش را - به‌هر روش ممکن - دارد و در این راه، آموزش کاربران تاثیر به‌سزایی بر کار می‌گذارد. البته بانک هم در جایگاه خودش مسوول برقراری امنیت سرورهایش است. امنیت فراتر از همه

هزینه‌ها و خطرات است. در یک سیستم بانکداری الکترونیکی - تا زمانی که یک حداقل محافظتی انجام شود - هزینه‌های برقراری امنیت در دستگاه کاربر تا جای ممکن، کاهش می‌یابد. یک روش و یک نفر به‌تنهایی نمی‌تواند امنیت را برقرار کند و همه باید روش‌های گوناگون را بیازمایند؛ هرچند که برخی از آن‌ها خطا باشد.

۷-۳- برای تحقیقات آینده

پس از بررسی راه های تأیید مشتری توسط بانکهای الکترونیکی و برای افزایش کیفیت خدمات بانکهای الکترونیک پیشنهادهای زیر مطرح می گردد:

♦- تدوین برنامه های راهبردی برای توسعه بانکداری الکترونیک.

♦- ارتقای سطح امنیت سیستمهای موجود و ترویج خدمات از طریق گسترش بانکهای اینترنتی.

♦- ایجاد یک سیستم یکپارچه برای سنجش اعتبار مشتری برای خدمات دهی به همه بانکهای کشور

منابع و مآخذ

♦- اکبری، فرشاد،(۱۳۸۵)، "**موانع رشد و توسعه تجارت الکترونیک در ایران**" دانشگاه شیراز

♦- رحیمی مقدم، علیرضا، (۱۳۸۷) ،" **تأیید اعتبار مشتری در بانکداری الکترونیک**"، بانک ملی، شماره ۱۴۷، ص ۱۸-۲۱.

♦- رحیمی مقدم، علیرضا، (۱۳۸۷) ،"**امنیت اطلاعات در بانکداری الکترونیک**"، بانک ملی، شماره ۱۴۶، ص ۱۵-۱۸.

♦- جلیلی، محمد، (۱۳۸۸) **گفتگو با بینا** ، شبکه اطلاع رسانی بانک و بیمه.

♦- چشم پنام، مسیب؛ (۱۳۸۵)، **"امنیت سیستم های بانکداری الکترونیکی امروزی"**، سایت بانک نوین.

♦- حمیدی زاده، محمد رضا ; قره چی، منیژه ; عبدالباقی، عبدالحمید(۱۳۸۶) "**بررسی عوامل زمینه ساز، چالشها و تنگناهای توسعه بانکداری الکترونیک**" ، پژوهش نامه علوم انسانی و اجتماعی، شماره ۲۳، ص۳۵-۵۴.

♦- محمودزاده،ابراهیم; رادرجبی، مهدی(۱۳۸۵)،"**مدیریت امنیت در سیستمهای اطلاعاتی**"،فصلنامه علوم مدیریت ایران، شماره ۴ ص۷۸-۱۱۲.

♦- Chaum, David. Scientific American. August 1992. pp.137-42

♦-Crede, Andereas (1999) Electronic Commerce and Industry: The Requirement and Opportunities for New Payment System Using the Internet, Scince Policy Research Unit University, p.17-19

♦-Fridgen, Michael & Schackmann, Jurgen & Volkert, Stefan (2001An Emperical Study, International Journal of Information

♦- Preference based Customer Models for Electronic Bankin University of Augsburg, Business School, Department of Information systems, Unversit tsstra e 16, 86135 Augsburg, Germany

♦-Liao, Shaoyi & et at. (1999) The Adoption of Virtual Banking: and Consumer Attitude, Information Management, No. 39, p. 283-

Pennathar, Anita K. (2001) E-Risk Management for Banks in Age of the Internet, Journal of Banking & Finance, No.25,p.2013-

♦- 2123.Availableat:www.elsevier.com/locate/enconbase

3.Internet Banking