

حفظ حریم خصوصی در بانکداری ابری



محمد مهدی واعظی نژاد
کارشناس امنیت اطلاعات
پژوهشکده پردازش هوشمند علایم

اشاره

امروزه به کارگیری الگوی رایانش ابری (Cloud Computing) که به روزترین و پیشرفته‌ترین فناوری در زمینه زیرساخت‌های فناوری اطلاعات به شمار می‌رود، با برخورداری از قابلیت‌های پویای خویش، معمول‌ترین روش برای اشتراک گذاری و مدیریت منابع فناوری اطلاعات است که در کشورهای توسعه یافته جهان، زیرساخت‌های آن در حال توسعه بوده و خدمات مبتنی بر ابر نیز با سرعت، رو به گسترش است. در این مطلب، پس از تعریف مفاهیم مهم و اساسی رایانش ابری، مسایل مرتبط با امنیت سیستم‌ها و تجهیزات بانکی، حفظ حریم خصوصی مشتریان و دست اندرکاران امور بانکداری، دسترسی و مدیریت امن حساب‌های بانکی، بر اساس استانداردهای ایزو ۲۷۰۰۱ و ۲۷۰۰۲ بررسی شده است.

رایانش ابری، یک فناوری جدید و به عبارتی بهتر، یک نگرش صحیح در پروژه‌های سرمایه گذاری فناوری اطلاعات است که علاوه بر کاهش هزینه‌ها، عملکرد بهتر و قابلیت‌های فراوانی را به ارمغان آورده است. این فناوری، راهی برای تغییر مدل‌های کسب و کار نبوده، بلکه همچون پدیده اینترنت، انقلابی در زیرساخت‌های فناوری اطلاعات قلمداد می‌شود که معماری نوینی را در توسعه، استقرار، اجرا و ارائه خدمات به همراه داشته است.

هم اکنون، شرکت‌های بزرگی مثل مایکروسافت، گوگل و آمازون، علاوه بر ارائه نرم افزارهای مبتنی بر ابر، اعلام کرده‌اند که اهداف آتی آنها، انتقال برنامه‌های کاربردی به محیط‌های ابری خواهد بود. برنامه‌هایی که بر روی ابرها مستقر شده و به راحتی، همچون ابر، بر روی سرورهای پیشرفته شناور هستند. پایگاه‌های داده ابری، تحول بزرگی را در تمرکز داده‌ها و اطلاعات ایجاد نموده‌اند.

با گسترش روز افزون خدمات مبتنی بر ابر، بانک‌ها و مؤسسات مالی نیز به دلیل ماهیت ساختاری خویش، تمایل دو چندانی به بهره‌گیری از مزایای این فناوری پیدا کرده‌اند. به فراخور این گرایش، ایجاد یک محیط امن بانکداری در بسترهای ابری که مورد تأیید کارشناسان بانکی و همچنین متخصصان امنیت فناوری اطلاعات باشد، بیش از پیش نمایان است. توجه به بانکداری ابری، به خصوص در چشم انداز فراگیر دیجیتال خدمات بانکداری الکترونیک برای بهبود ایمنی، کیفیت خدمات و کاهش هزینه‌های بانکداری، ضروری است. بنابراین نگاه جدی به این مقوله، ضمن ایجاد تعامل مناسب میان بانک‌ها باعث می‌شود تا نظام بانکی کشور به پتانسیل‌های لازم جهت تحول در ارائه خدمات نوین بانکداری با کیفیت بالا و هزینه‌های مقرون به صرفه نایل شود.

رایانش ابری در صنعت بانکداری

از مهمترین ضعف‌های نظام بانکداری به شیوه سنتی، می‌توان به هزینه زیاد و بهره‌وری پایین در استفاده از امکانات اشاره نمود که ضمن تحمیل هزینه‌های گزاف به بانک‌ها، امکان بهره‌مندی از آن بسیار پایین بوده و در عمل، در بسیاری از موارد، علی‌رغم تلاش‌های بسیار، شکایات زیادی را از سوی مشتریان به همراه داشته است.

در رایانش ابری، بانک‌ها می‌توانند ضمن کاهش هزینه‌ها، از طریق ادغام سیستم‌ها و تجهیزات سخت افزاری و به اشتراک گذاری آنها بر اساس نیاز کاربران، یک محیط پویا را در ارائه خدمات بانکداری ایجاد نمایند که علاوه بر مالکیت سیستم، هزینه‌های تعمیر و نگهداری آن، تهیه نسخه‌های پشتیبان از اطلاعات و استخدام کارشناسان فنی، به ارائه دهندگان خدمات ابری واگذار می‌شود.

همزمان با رشد و گسترش این فناوری،

استانداردهای مخصوص به آن نیز در حوزه بانکداری، در حال تدوین و اجرا است که هدف آنها بیشتر بر روی چگونگی نگهداری سوابق تراکنش‌های مالی، نحوه نظارت بر مشتریان و کاربران، مدیریت حساب‌های بانکی و نحوه همکاری مؤسسات مالی برای ارائه خدمات بانکی کارآمد و مؤثر و همچنین تحلیل و بررسی قاعده‌مند داده‌های نظام بانکداری الکترونیک، متمرکز شده است.

پیش بینی می‌شود با حرکت و انتقال نرم افزارهای بانکی به الگوهای مبتنی بر رایانش ابری و مدیریت آنها از طریق ابرها، انقلابی در ارائه خدمات بانکداری به وقوع بپیوندد که نتایج آن، امکان دسترسی به این خدمات را برای همگان و در همه جا فراهم ساخته و علاوه بر کاهش شدید هزینه‌ها، گام‌های اساسی برای بهره‌مندی از نظام الگومند بانکداری فراهم شود که جهت رفاه حال مشتریان، با فناوری ادغام، همگام و همسو شده است.

امنیت در مدل‌های بانکداری ابری

بر اساس مدل‌های سرویس ابری، ارائه دهندگان خدمات بانکداری ابری به سه دسته تقسیم می‌شوند:

۱- برنامه‌های کاربردی در ابر (نرم افزار به عنوان یک سرویس - SaaS): در این مدل، برنامه‌های بانکی از طریق یک رابط کاربری سبک مانند مرورگر وب، بر روی زیرساخت‌های ابری، اجرا می‌شوند.

در این نوع از خدمات ابری، امنیت و حفاظت از حریم خصوصی، به عنوان بخشی جدایی ناپذیر از SaaS، به دریافت کنندگان خدمات ارائه می‌شود.

۲- سیستم عامل در ابر (پلت فرم به عنوان یک سرویس - PaaS): این مدل، توانایی استقرار یا به دست آوردن برنامه‌های نوشته شده با استفاده از زبان‌های برنامه نویسی و ابزارهای پشتیبانی آن را توسط ارائه دهنده خدمات ابری، به دریافت کنندگان ارائه می‌دهد. در این مدل، برنامه‌های کاربردی مورد استفاده، قابل پیکربندی و کنترل بوده و تلاش می‌شود تا با مکانیزم‌های امنیتی اساسی در ارائه خدمات ابری مانند رمزگذاری اطلاعات، تأیید هویت و مجوزهای لازم و همچنین در سطح برنامه‌های کاربردی، با تعیین میزان دسترسی و کنترل آن، سازوکارهای حفاظتی لازم برای تأمین امنیت و حفظ حریم خصوصی به عمل آید.

۳- زیرساخت در ابر (زیرساخت به عنوان یک سرویس - IaaS): در این مدل، پردازش، ذخیره سازی، کنترل محدود امور شبکه‌ای (مانند فایروال‌ها)، بعضی از منابع محاسباتی، اجرا و کنترل نرم افزارهای دلخواه شامل سیستم عامل و برنامه‌های کاربردی، توسط دریافت کنندگان خدمات ابری، قابل تنظیم است. در این نوع از خدمات ابری، توسعه دهندگان نرم افزارهای بانکی، مسئول کامل حفاظت از امنیت و حفظ حریم خصوصی دریافت کنندگان خدمات، به شمار می‌روند.

حفظ حریم خصوصی در بانکداری ابری

در چند سال گذشته، تحقیقات فراوانی بر روی مسائل امنیتی و حفظ حریم خصوصی در سیستم‌های اطلاعاتی بانک‌ها انجام شده است. انجمن‌های ملی و بین‌المللی مختلفی نیز برای بررسی مسائل مرتبط با حفاظت از داده‌ها و امنیت در محیط‌های مالی تشکیل شده‌اند که به طور عمده، بر روی امنیت در سیستم‌های بانکی و ارائه راه حل‌های امنیتی مشترک، متمرکز شده‌اند. این انجمن‌ها، طیف گسترده‌ای از مسائل امنیتی در خدمات بانکداری را مورد بررسی قرار داده و دستورالعمل‌های عملی برای ایجاد و ارایه خدمات بانکداری امن منتشر کرده‌اند.

از آنجا که امنیت و حفظ حریم خصوصی و همچنین حفاظت از اطلاعات مشتریان، در دسترسی امن به داده‌های مالی در ابر از بالاترین درجه اهمیت برخوردار است، می‌توان سه اصل مهم را برای اطمینان از حفظ حریم خصوصی، صحت محتوا و قابلیت اعتماد، در نظر گرفت.

۲. ممکن است یک بانک، مشتریانی در بانک‌های مختلف داشته باشد، لازم است از طریق مکانیزم‌های احراز هویت، دسترسی آن به مدارک مشتریان امکان‌پذیر شود. صحت اطلاعات نیز، پس از پایان بررسی حساب مشتری، باید به تأیید بانک برسد.

۳. در مواردی که اطلاعات مالی در بانک‌های مختلف به اشتراک گذاشته می‌شود، باید مالکیت این اطلاعات به صورت دقیق و شفاف مشخص بوده و مالک آن، تمامی الزامات امنیتی را در این خصوص به عمل آورد.

۴. استفاده از گواهینامه‌های SSL و پروتکل‌های رمزنگاری اطلاعات برای تأمین امنیت داده‌های در حال انتقال در طول شبکه‌های عمومی نظیر اینترنت، توسط بانک‌ها باید اجرا شود.

۵. با استفاده از روش‌هایی همچون امضای دیجیتال و رمزگذاری اطلاعات، باید مانع انکار اطلاعات توسط افراد دخیل در امر خدمات بانکداری شد.

۶. در سیستم خدمات بانکداری، اطلاعات باید از



۱- تمامی تراکنش‌ها و ارتباطات مالی باید از طریق رمزنگاری توسط مالکان آنها، کنترل، محافظت، ذخیره سازی، انتقال و مورد دسترسی امن قرار گیرند.

۲- در ایجاد و نگهداری اطلاعات باید اصالت محتوا و جامعیت داده‌ها با توجه به امکان سفرهای ساختن حفظ حریم خصوصی مشتریان در فرآیندهای ادغام حساب‌های بانکی در نظر گرفته شود.

۳- دسترسی و به اشتراک گذاری اطلاعات مالی باید از طریق امضای دیجیتال و فرآیندهای صدور گواهینامه، جهت جلوگیری از تغییرات غیرمجاز در محتوای اطلاعات حساس مالی، صورت گیرد.

الزامات امنیتی

اگرچه بعضی از نیازهای امنیتی و حفظ حریم خصوصی در برنامه‌های بانکداری ابری به مدل سرویس یا استقرار ابر مورد استفاده، بستگی دارد، در زیر به برخی از مهم‌ترین موارد اشاره می‌شود:

۱. دسترسی به اطلاعات حساب‌ها باید از طریق یک روال کنترل شده و بر اساس مجوزهای لازم صورت گیرد.

لازم توسط بانک‌ها به عمل آید.

۱۱. لازم است که اطلاعات مالی در فرمت‌های خاصی تهیه شوند که قابل استفاده در تمام سیستم‌های بانکی بوده و مشکلی به نام عدم انطباق اطلاعات در فرآیندهای بانکداری، هرگز به وقوع نپیوندد.

۱۲. دسترسی به اطلاعات رمزنگاری شده در سیستم‌های بانکی، از طریق مکانیزم‌های رمزگشایی مبتنی بر هویت و اخذ مجوز بر اساس کلیدهای خصوصی صورت گیرد.

۱۳. سروورها باید در مکان‌های ایمن نگهداری شوند که کنترل دسترسی به آنها به صورت امن صورت می‌پذیرد.

۱۴. رمزنگاری داده‌ها در حین ذخیره سازی و انتقال اطلاعات همواره در جریان باشد و هیچ فردی، قادر به دخالت در این امر نباشد.

۱۵. دسترسی‌ها، بر اساس مجموعه‌ای از کنترل‌های مبتنی بر نقش و یا سیاست‌های مبتنی بر ویژگی، شکل گرفته و اعمال شوند.

۱۶. سیاست‌های امنیتی لحاظ شده در بانکداری ابری، توسط پارامترهای قابل سنجش، در فواصل زمانی مشخص ارزیابی گردند.

۱۷. تمامی ارتباطات و فرآیندهای میان بانک‌ها باید به صورت امنی که از طریق الگوریتم‌های رمزنگاری، پروتکل‌ها و گواهینامه‌های امنیتی همچون SSL، TLS و IPsec حاصل می‌شود، صورت بگیرد تا اطمینان حاصل شود که اطلاعات در حال انتقال، از شنود و دستکاری غیرمجاز در شبکه‌های عمومی، محفوظ هستند.

نتیجه گیری:

در این مقاله، تحلیل مختصری از مخاطرات امنیتی که می‌تواند بانکداری ابری را تحت تأثیر خویش قرار دهد، ارائه شد و راه‌های حفاظت از آنها به نحوی که در عین استفاده از آن، خدمات بانکداری نیز به نحو مطلوبی انجام شود، ذکر گردید.

به طور خلاصه، باید اذعان داشت که امنیت و حفظ حریم خصوصی، چیزی بسیار فراتر از اجرای دسترسی‌های کاربری و رمزهای عبور بوده و به کارگیری و اعمال الزامات امنیتی، یک ضرورت بزرگ برای بانک‌ها است که از اطلاعات حساس و حیاتی برخوردار هستند. با اجرای دقیق یک مدل مبتنی بر ابر، می‌توان بالاترین سطوح امنیت فیزیکی، شبکه‌ای، برنامه‌های کاربردی، داده‌ها و سیستم‌های داخلی را تضمین نمود که استراتژی‌هایی همچون تهیه نسخه‌های پشتیبان از اطلاعات، روش‌ها و سیاست‌های امن داخلی، شیوه‌های استاندارد تنظیمات امنیتی و صدور گواهینامه‌ها نیز در بطن آن گنجانده شده است. در این مدل، موارد مهمی همچون رمزنگاری اطلاعات و احراز هویت کاربران و مشتریان نیز به طور مرتب در حال اجرا است.

یکپارچگی و جامعیت به معنای حفظ دقت، صحت و قوام داده‌ها برخوردار بوده و از دستکاری غیرمجاز، مصون بمانند. همچنین محرمانگی این اطلاعات نیز طبق استاندارد ایزو ۲۷۰۰۱ تضمین شود که این امر نیز، به کمک روش‌های رمزنگاری امکان پذیر است.

۷. سیستم‌های خدمات بانکداری، در فواصل زمانی معین جهت اطمینان از صحت عملکرد و رعایت نکات امنیتی لحاظ شده، توسط کارشناسان مربوطه، مورد ممیزی قرار گیرند.

۸. تهیه نسخه‌های پشتیبان از اطلاعات، بر اساس قواعد مشخص، توسط بانک‌ها صورت پذیرد.

۹. کنترل‌های امنیتی لازم برای هنگامی که یکی از کاربران سیستم بانکی، تغییر شغل یافته و یا از سازمان اخراج می‌گردد، اعمال گردد تا از افشای تغییرات ناخواسته و نامجاز در سیستم جلوگیری شود.

۱۰. امضای دیجیتال یک ابزار بسیار مفید برای ارایه صحت، صداقت و عدم انکار است. باید از هویت امضا کننده جهت استراق سمع و موارد دیگر، حفاظت‌های