عنوان[1] (بانکداری هوشمند، مشتری محفوظ: تحلیل ریسک‌های امنیتی و راهکارهای حفاظتی در اپلیکیشین های موبایل بانک)

نویسنده اول[2] : حمید رنجر

تاریخ ارسال: ۱۴۰۴/۰۹/۲۵

نام و نام خانوادگی: حمید رنجبر
کد پرسنلی: ۰۰۴۲۳۲
کد ملی: ۰۶۳۹۸۴۴۳۲۴
محل خدمت: خراسان شمالی شعبه گرمه
شماره همراه: ۰۹۱۵۳۷۲۸۲۵۴

[1] سازمان: بانک قرض الحسنه مهر ایران.
[2] کارمند بانک قرض الحسنه مهر ایران.

چکیده:

همانطور که می‌دانید صیانت از مشتریان از ارکان اساسی ثبات و سلامت مالی و از رویکردهای اصلی نظام بانک مرکزی کشور است. همچنین مسئله اعتماد عمومی، رعایت عدالت و شفافیت، محرمانگی اطلاعات مالی مشتریان و پیشگیری از آسیب‌های اجتماعی و اقتصادی از مهمترین اهداف این رویکرد است. در این پژوهش ابتدا به تبیین کلیات کلیدواژه مساله پرداخته شده است و در ادامه مطالب اطلاعاتی در رابطه با موضوع بیان شده و به تحلیل مسائل پرداخته شده است و در انتها راهکارهایی برای کمک به حل مساله ارائه گردیده است. امید است که تحلیل پیش رو کمکی به حل مساله صیانت از حریم شخصی مشتریان همزمان با پیشرفت روز افزون مسائل بانکی در کشور عزیزمان کند.

واژه‌های کلیدی: بانکداری هوشمند-حریم خصوصی-اپلیکیشن موبایل بانک-امنیت سایبری-تهدیدات امنیتی-صیانت از مشتریان.

طبقه‌بندی JEL:

G۲۱ - Banks; Depository Institutions; Micro Finance Institutions; Mortgages
G۲۸ - Financial Institutions and Services: Government Policy and Regulation
O۳۳ - Technological Change: Choices and Consequences; Diffusion Processes
G۱۸ - Financial Markets and Institutions: Government Policy and Regulation
G۱٤ - Information and Market Efficiency; Event Studies; Insider Trading

۱. مقدمه

در عصر دیجیتال تلفن همراه به قلب تپنده زندگی انسان تبدیل شده و بانکداری نیز از این تحول بی‌بهره نمانده است. اپلیکیشن‌های موبایل بانک با شعار سهولت، سرعت و دسترسی همیشگی در کانون رابطه بانک و مشتری قرار گرفته‌اند. این تحول نه تنها روش‌های انجام تراکنش‌ها را متحول کرده، بلکه خود به یک «کیف پول هوشمند» همه‌کاره تبدیل شده است که از پرداخت قبوض تا سرمایه‌گذاری را در بر می‌گیرد. با این حال، این تمرکز روزافزون امور مالی حساس در یک دستگاه کوچک دیجیتال، سوال حیاتی را در ذهن انسان روشن می‌کند: آیا این «هوشمندی» به همان میزان که خدمات را بهبود مي بخشد از دارايي و حريم خصوصي مشتري نيز صيانت مي كند؟

گسترش نفوذ موبایل بانک‌ها، سطح مواجهه کاربران را با تهدیدات سایبری به شکلی بی‌سابقه گسترش داده است. در حالی که بانک‌ها با ارائه ویژگی‌های نوین مانند پرداخت با QR، احراز هویت با اثر انگشت و... به خدمات غیرحضوری به رقابتی تنگاتنگ مشغولند، همواره این نگرانی وجود دارد که «امنیت» در این مسیر پرشتاب، ممکن است به عنوان یک «مزیت رقابتی ثانویه» و نه یک «پایه اساسی» در نظر گرفته شود. از سوی دیگر، مشتریان نیز در هیجان دسترسی آسان، اغلب از پیچیدگی‌های ریسک‌های امنیتی مرتبط بی‌خبرند.

مقاله حاضر با عنوان «بانکداری هوشمند، مشتری محفوظ: تحلیل ریسک‌های امنیتی و راهکارهاي حفاظتي در اپليكيشين هاي موبايل بانك» درپي پاسخ به اين ضرورت دوگانه است. اين پژوهش برآن است تا با عبور از نگاه سطحي به امنيت، به تحليل ساختار يافته ريسك هاي امنيتي ذاتي در بستر موبايل بانك ها بپردازد.

سوال اصلي اين است كه مهم ترين تهديدات امنيتي پيش روي كاربران اپليكيشن هاي موبايل بانك چيست و چه راهكارهاي حفاظتي چندلايه اي را مي توان در سطوح فني انساني و مقرراتي تدوين كرد؟

هدف از اين مقاله ارائه تصويري روشن از چالش هاي امنيتي در بانكداري موبايلي و تبيين راهكارهايي است كه نه تنها براي متخصصان فني، بلكه براي سياست گذاران، مديران بانكي و آحاد كاربران قابل درك و اجرا باشد.

در اين مسير به بررسي چالش هايي از جمله چالش هاي فناورانه و امنيتي، قانوني و نظارتي، رفتاري و اجتماعي، اقتصادي و تجاري، چالش هاي نوظهور و آينده نگر و چالش هاي خاص براي كشور عزيزمان ايران پرداخته و در مقابل راهكارهايي براي حفظ حريم خصوصي در بانكداري هوشمند ارائه مي گردد.

اميد است يافته هاي اين تحليل گامي در جهت تحقق شعار (بانكداري هوشمند، مشتري محفوظ) برداشته و به ايجاد اكوسيستم مالي ديجيتالي امن تر و قابل اعتمادتر در كشورمان كمك نمايد.

۲. تعاریف و مبانی نظری

۱،۲. مفهوم بانکداری هوشمند

بانکداری هوشمند به مدلی از ارائه خدمات مالی اطلاق می‌شود که با اتکا به فناوری‌های دیجیتال نوین، خدمات بانکی را به‌صورت سریع، شخصی‌سازی‌شده و امن در اختیار مشتریان قرار می‌دهد. این مدل بر دیجیتال‌سازی کامل فرآیندها، تحلیل هوشمند داده‌های مشتری و ادغام امنیت در طراحی سیستم‌ها استوار است.

از منظر فناوری اطلاعات، بانکداری هوشمند یک اکوسیستم یکپارچه است که از کلان‌داده، هوش مصنوعی و الگوریتم‌های پیش‌بینانه برای ارائه خدماتی همچون وام‌دهی هوشمند، مدیریت سرمایه و تشخیص تقلب استفاده می‌کند. از دیدگاه امنیت سایبری، هوشمندی این نظام در توانایی پیش‌بینی، شناسایی و خنثی‌سازی تهدیدات نیز تجلی می‌یابد.

۲,۲. مفهوم حریم خصوصی در دنیای دیجیتال

حریم خصوصی دیجیتال به حق افراد برای کنترل نحوه جمع‌آوری، استفاده، افشا و نگهداری اطلاعات شخصی‌شان در فضای دیجیتال اشاره دارد. این مفهوم ابعاد حقوقی، اجتماعی و فنی را در بر می‌گیرد و در حوزه بانکداری دیجیتال به‌طور خاص بر حفاظت از داده‌های مالی، تراکنش‌ها، رفتارهای مصرفی و ترجیحات مشتری تمرکز دارد.

حریم خصوصی مشتری در خدمات مالی دیجیتال مستلزم شفافیت، رضایت آگاهانه، حداقل‌سازی داده‌ها و استفاده از سازوکارهای فنی مؤثر برای جلوگیری از دسترسی غیرمجاز است.

۳. مروری بر تحقیقات پیشین

۱,۳. تحقیقات خارجی

مطالعات بین‌المللی نشان می‌دهند که دیجیتالی شدن بانکداری موجب افزایش ریسک‌هایی نظیر سرقت هویت، کلاهبرداری مالی، اشتراک داده بدون رضایت آگاهانه، نقض داده‌های حساس و پروفایل‌سازی رفتاری تهاجمی شده است. همچنین، توسعه بانکداری باز و استفاده گسترده از APIها، چالش‌های جدیدی در حوزه امنیت و مسئولیت‌پذیری ایجاد کرده است.

۲,۳. تحقیقات داخلی

پژوهش‌های داخلی عمدتاً بر چالش‌هایی مانند فقدان قانون جامع حفاظت از داده، سطح پایین آگاهی کاربران، آسیب‌پذیری اپلیکیشن‌های بانکی و محدودیت‌های ناشی از تحریم‌ها تمرکز دارند. نتایج این مطالعات نشان می‌دهد که بانک‌های ایرانی اغلب بیش از نیاز واقعی داده جمع‌آوری می‌کنند و شفافیت کافی در سیاست‌های اشتراک داده وجود ندارد.

٤. فناوری‌های بانکداری هوشمند و حوزه‌های جمع‌آوری داده

۱,٤. فناوری‌های کلیدی

بانکداری باز، هوش مصنوعی، فین‌تک‌ها، پرداخت‌های دیجیتال، چت‌بات‌ها و دستیاران هوشمند از جمله فناوری‌هایی هستند که نقش اساسی در بانکداری هوشمند ایفا می‌کنند. این فناوری‌ها داده‌هایی فراتر از اطلاعات مالی سنتی، از جمله داده‌های رفتاری، مکانی، بیومتریک و روان‌شناختی را جمع‌آوری می‌کنند.

۲,٤. حوزه‌های اصلی داده

داده‌های مالی، رفتاری، مکانی، بیومتریک، اجتماعی، فرافکنشی و وابستگی، مهم‌ترین انواع داده‌هایی هستند که در بانکداری هوشمند مورد استفاده قرار می‌گیرند. تحلیل ترکیبی این داده‌ها قدرت پیش‌بینی بالایی ایجاد می‌کند، اما همزمان ریسک‌های جدی برای حریم خصوصی به همراه دارد.

۳,٤. چالش‌های خاص ایران

جمع‌آوری داده‌های اضافی، ذخیره‌سازی متمرکز، اشتراک غیرشفاف داده با نهادهای مختلف و ضعف زیرساخت‌های رمزنگاری از مهم‌ترین چالش‌های بومی ایران در این حوزه محسوب می‌شوند.

۵. چالش‌های حریم خصوصی در بانکداری هوشمند

۵,۱. چالش‌های فناورانه و امنیتی

پیچیدگی زنجیره تأمین فناوری، ناامنی APIها، آسیب‌پذیری‌های هوش مصنوعی و خطر استنتاج معکوس از داده‌ها از جمله چالش‌های مهم این حوزه هستند.

۵,۲. چالش‌های قانونی و نظارتی

پراکندگی قوانین، تعارض منافع بین نهادهای نظارتی، و ابهام در مسئولیت نقض حریم خصوصی در اکوسیستم فین‌تک، چالش‌های اساسی در سطح مقرراتی ایجاد کرده‌اند.

۵,۳. چالش‌های رفتاری و اجتماعی

پارادوکس حریم خصوصی، شکاف سواد دیجیتال و فشار اجتماعی برای اشتراک‌گذاری داده‌ها، نقش مهمی در تضعیف حفاظت مؤثر از حریم خصوصی ایفا می‌کنند.

۵,٤. چالش‌های اقتصادی و تجاری

مدل‌های تجاری مبتنی بر داده، هزینه‌های بالای انطباق مقرراتی و رقابت نابرابر با غول‌های فناوری، بانک‌ها را در موقعیتی پیچیده قرار داده‌اند.

۵,۵. چالش‌های نوظهور و آینده‌نگر

رایانش کوانتومی، متاورس و اینترنت اشیای مالی، افق‌های جدیدی از ریسک‌های حریم خصوصی را پیش روی بانکداری هوشمند قرار می‌دهند.

۵,٦. چالش‌های خاص ایران

تحریم‌ها، الزامات گسترده اشتراک داده با نهادهای حاکمیتی و استفاده از سامانه‌های قدیمی، ریسک‌های مضاعفی برای حریم خصوصی مشتریان ایرانی ایجاد کرده‌اند.

٦. راهکارهای حفظ حریم خصوصی در بانکداری هوشمند

٦,١. راهکارهای فناورانه

طراحی با حریم خصوصی، استفاده از رمزنگاری پیشرفته، معماری‌های غیرمتمرکز، یادگیری فدرال و فناوری‌های مقاوم در برابر کوانتوم از مهم‌ترین راهکارهای فنی محسوب می‌شوند.

٦,٢. راهکارهای قانونی و نظارتی

تدوین قانون جامع حفاظت از داده، ایجاد نهاد نظارتی مستقل، حسابرسی‌های منظم و افزایش شفافیت، بستر حقوقی حفاظت از حریم خصوصی را تقویت می‌کند.

٦,٣. راهکارهای کاربرمحور

ایجاد داشبوردهای کنترل حریم خصوصی، مدیریت رضایت پویا، افزایش سواد دیجیتال و طراحی رابط کاربری شفاف از جمله اقدامات مؤثر در توانمندسازی کاربران است.

٦,٤. راهکارهای همکاری صنعتی و بین‌المللی

استانداردهای مشترک، اتحادیه‌های امنیتی و همکاری‌های پژوهشی بین‌المللی نقش مهمی در ارتقای سطح حفاظت ایفا می‌کنند.

٦,٥. راهکارهای ویژه ایران

توسعه فناوری‌های بومی امن، چارچوب قانونی متناسب با شرایط کشور و اجرای برنامه‌های انتقال تدریجی برای بانک‌ها ضروری است.

٧. نتیجه‌گیری نهایی

حفظ حریم خصوصی در بانکداری هوشمند نیازمند رویکردی چندلایه، پویا و مستمر است. تحقق این هدف مستلزم ترکیب راهکارهای فنی، قانونی، فرهنگی و مدیریتی و به‌روزرسانی مداوم آن‌ها متناسب با تحولات فناوری است. در شرایط ایران، توجه همزمان به استانداردهای بین‌المللی و ملاحظات بومی اهمیت ویژه‌ای دارد. موفقیت این مسیر در گرو تعهد مدیران ارشد، سرمایه‌گذاری هدفمند، آموزش مستمر و همکاری همه ذی‌نفعان نظام مالی است.

۸.پیشنهادهای کاربردی

۱. الزام طراحی مبتنی بر حریم خصوصی در توسعه اپلیکیشن‌های بانکی
۲. بانک‌ها موظف شوند اصول «طراحی با حریم خصوصی» را به‌عنوان یک الزام فنی در تمام چرخه عمر توسعه نرم‌افزار (SDLC) اعمال کرده و تأیید رعایت این اصول را پیش از انتشار هر نسخه جدید اخذ کنند.
۳. ایجاد داشبورد شفاف مدیریت داده برای مشتریان
٤. در اپلیکیشن‌های موبایل‌بانک بخشی اختصاصی برای نمایش، مدیریت و محدودسازی داده‌های ذخیره‌شده هر مشتری ایجاد شود تا کاربران بتوانند نوع داده، هدف استفاده و سطح اشتراک‌گذاری آن را به‌صورت پویا کنترل کنند.
٥. پیاده‌سازی مدیریت رضایت آگاهانه و پویا (Dynamic Consent)
٦. رضایت مشتریان از حالت کلی و یک‌باره خارج شده و به رضایت‌های موضوع‌محور، زمان‌دار و قابل لغو در هر زمان تبدیل شود؛ به‌گونه‌ای که هر کاربرد داده نیازمند رضایت مستقل باشد.
۷. کاهش جمع‌آوری داده‌های غیرضروری در خدمات بانکی
۸. بانک‌ها با بازنگری فرآیندهای افتتاح حساب و ارائه خدمات دیجیتال، جمع‌آوری داده‌ها را به حداقل داده‌های ضروری محدود کرده و حذف داده‌های مازاد را در دستور کار قرار دهند.
۹. الزام حسابرسی دوره‌ای حریم خصوصی و امنیت داده
۱۰. حسابرسی‌های مستقل و منظم در حوزه امنیت اطلاعات و حریم خصوصی انجام شده و خلاصه نتایج آن به‌صورت عمومی منتشر شود تا پاسخگویی و اعتماد عمومی تقویت گردد.
۱۱. تفکیک و طبقه‌بندی داده‌های حساس در معماری سامانه‌ها
۱۲. داده‌های مالی، بیومتریک و رفتاری در لایه‌های جداگانه و با سطوح دسترسی متفاوت ذخیره‌سازی شوند تا در صورت بروز رخداد امنیتی، دامنه آسیب محدود گردد.
۱۳. استفاده از فناوری‌های حفظکننده حریم خصوصی در تحلیل داده‌ها
۱٤. در تحلیل‌های کلان و امتیازدهی اعتباری، از فناوری‌هایی مانند حریم خصوصی تفاضلی، یادگیری فدرال و محاسبات امن چندجانبه به‌جای پردازش متمرکز داده‌های خام استفاده شود.
۱٥. تدوین دستورالعمل شفاف اشتراک داده با اشخاص ثالث
۱٦. چارچوب‌های مشخص برای اشتراک داده با فین‌تک‌ها و نهادهای همکار تدوین شود که شامل حدود دسترسی، مدت نگهداری داده، مسئولیت نقض حریم خصوصی و سازوکار پاسخگویی باشد.
۱۷. آموزش تخصصی کارکنان بانکی و توسعه‌دهندگان نرم‌افزار
۱۸. برنامه‌های آموزشی مستمر در زمینه امنیت سایبری، حریم خصوصی و اخلاق داده برای کارکنان بانک‌ها و تیم‌های فنی اجرا شود تا خطاهای انسانی کاهش یابد.
۱۹. ارتقای سواد حریم خصوصی کاربران بانکی
۲۰. بانک‌ها با تولید محتوای آموزشی ساده، پیام‌های هشدار هوشمند در اپلیکیشن و شبیه‌سازهای تعاملی، آگاهی کاربران از ریسک‌های امنیتی و حقوق حریم خصوصی را افزایش دهند.
۲۱. ایجاد مرکز پاسخگویی به رخدادهای نقض حریم خصوصی
۲۲. واحدی تخصصی برای دریافت، بررسی و پاسخ سریع به شکایات و رخدادهای نقض حریم خصوصی مشتریان ایجاد شود و زمان پاسخگویی مشخص و الزام‌آور باشد.
۲۳. توسعه و استفاده از راهکارهای بومی امنیت داده

۲۴. با توجه به محدودیت‌های بین‌المللی، سرمایه‌گذاری هدفمند در توسعه ابزارها و الگوریتم‌های بومی رمزنگاری و مدیریت هویت دیجیتال در دستور کار بانک‌ها قرار گیرد.

۲۵. پیاده‌سازی گزارش‌های شفافیت داده‌ای برای عموم

۲۶. بانک‌ها به‌صورت دوره‌ای گزارش‌هایی درباره نحوه استفاده از داده‌ها، درخواست‌های نهادی برای دسترسی به اطلاعات و رخدادهای امنیتی منتشر کنند.

۲۷. اجرای تدریجی استانداردهای پیشرفته متناسب با توان بانک‌ها

۲۸. برای جلوگیری از فشار بیش‌ازحد بر بانک‌های کوچک، اجرای الزامات حریم خصوصی به‌صورت مرحله‌ای و با حمایت فنی و مالی نهادهای ناظر انجام شود.

۲۹. ایجاد سازوکار اعتراض و بازبینی تصمیمات الگوریتمی

۳۰. مشتریان باید امکان اعتراض به تصمیمات خودکار مانند رد تسهیلات یا امتیازدهی اعتباری را داشته باشند و فرآیند بازبینی انسانی به‌صورت شفاف تعریف شود.

۵. فهرست منابع

۱. European Central Bank (ECB). (۲۰۲۰). Report on Digital Transformation in Banking. ECB Publishing.
۲. Lee, I., & Shin, Y. J. (۲۰۱۸). Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, ۶۱(۱), ۳۵–۴۶.
۳. Khan, S., & Alqahtani, S. (۲۰۲۲). A framework for secure smart banking: Integrating AI and blockchain. Journal of Cybersecurity and Privacy, ۲(۳), ۵۱۲–۵۳۰.
۴. Federal Trade Commission (FTC). (۲۰۱۲). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. FTC Report.
۵. European Union. (۲۰۱۶). General Data Protection Regulation (GDPR). Regulation (EU) ۲۰۱۶/۶۷۹.
۶. Mittelstadt, B. D. (۲۰۱۹). AI ethics – Too principled to fail? Philosophy & Technology, ۳۲(۴), ۴۹۹–۵۱۲.
۷. Kumar, A., Lim, H., & Park, J. (۲۰۲۱). Data aggregation risks in fintech and digital banking. Journal of Financial Regulation and Compliance, ۲۹(۴), ۳۹۱–۴۰۸.
۸. Zarouali, B., Van den Broeck, E., Walrave, M., & Poels, K. (۲۰۲۱). Predicting consumer responses to personalized advertising: The role of data privacy concerns. Journal of Business Research, ۱۲۲, ۴۶۸–۴۸۰.
۹. Cavoukian, A. (۲۰۱۰). Privacy by Design: The ۷ Foundational Principles. Information and Privacy Commissioner of Ontario.
۱۰. Greenleaf, G. (۲۰۲۲). Global data privacy laws ۲۰۲۱: Despite COVID delays, ۱۴۵ laws show GDPR dominance. Privacy Laws & Business International Report, ۱۷۱, ۱–۶.

Title

Smart Banking, Protected Customer: An Analysis of Security Risks and Privacy Protection Mechanisms in Mobile Banking Applications

Authors

Hamid Ranger

Abstract

In the digital era, mobile banking applications have become a central component of modern financial systems by offering convenience, speed, and continuous access to banking services. While these applications significantly enhance customer experience and operational efficiency, they also concentrate vast amounts of sensitive financial, behavioral, and personal data within digital platforms, thereby increasing exposure to privacy and cybersecurity risks.

This paper aims to analyze the major security and privacy risks inherent in smart banking environments, with a specific focus on mobile banking applications. The study adopts a descriptive–analytical approach to examine technological, legal, behavioral, economic, and emerging challenges associated with data collection, processing, and sharing in smart banking ecosystems. Particular attention is given to context-specific challenges faced by developing financial systems, especially in Iran, including regulatory gaps, legacy infrastructures, technological constraints, and limited user awareness.

Based on the analysis, the paper proposes a set of multi-layered protection mechanisms encompassing technical solutions (such as privacy-by-design architectures, advanced cryptography, and privacy-preserving data analytics), regulatory and governance measures, and user-centered strategies aimed at enhancing privacy awareness and control. The findings highlight that effective protection of customer privacy in smart banking requires an integrated and adaptive approach that balances innovation, security, regulatory compliance, and public trust.

The study contributes to the existing literature by providing a comprehensive and practical framework that can assist policymakers, banking executives, system designers, and end-users in building a more secure and privacy-respecting digital banking ecosystem.

Keywords

Smart Banking; Mobile Banking Applications; Data Privacy; Cybersecurity Risks; Financial Technology (FinTech)

JEL Classification

G۲۱ – Banks; Depository Institutions; Micro Finance Institutions; Mortgages
G۲۸ – Financial Institutions and Services: Government Policy and Regulation
G۱۸ – Financial Markets and Institutions: Government Policy and Regulation
G۱٤ – Information and Market Efficiency; Event Studies; Insider Trading
O۳۳ – Technological Change: Choices and Consequences; Diffusion Processes