مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۸، زمستان ۱۳۹۶، ص ۱۲۹- ۱۱۸

ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال دوم)
شماره ۸ / زمستان ۱۳۹۶ / ص ۱۲۹- ۱۱۸

ایمن سازی پرداخت وجلوگیری از پولشویی و جرایم مالی با سیستم مبتنی بر شاخص‌های نوین بیومتریک

بهنوش داریوشی [۱]، عرفانه نوروزی [۲]

[۱] دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه آزاد اسلامی واحد سپیدان

[۲] گروه کامپیوتر واحد سپیدان، دانشگاه آزاد اسلامی واحد سپیدان

نام نویسنده مسئول:
بهنوش داریوشی

چکیده

همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی) ، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است . استفاده کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات ، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می باشند .امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله این مولفه ها بوده که نمی توان آن را مختص یک فرد یا سازمان در نظر گرفت . بیومتریک یک سیستم تشخیص الگو است که افراد را بر اساس ویژگی های منحصر به فرد و خاص فیزیولوژیکی یا رافتاری که دارد بصورت خودکار شناسائی میکند. ویژگی های بیومتریک را نمی توان امانت داد یا گرفت و همچنین نمی توان خرید و فراموش کرد و جعل کرد آن هم امروزه عملاً غیر ممکن است، بنابراین بصورت ذاتی نسبت به روش های رایج احراز هویت قابل اعتمادتر است. همچنین از آن ها می توان در کلیه امور جاری و در هر سطحی از کشور مانند دنیای فناوری اطلاعات و حتی دنیای الکترونیک نیز استفاده کرد. امروزه به علت اهمیت روز افزون اطلاعات و تمایل افراد به امنیت بیشتر اطلاعات مخصوصا در اینترنت ابزارهای قدیمی مانند استفاده از پسورد به تنهایی جوابگو و قابل اعتماد نمی باشد، خصوصا با ایجاد تجارت الکترونیک و خرید و فروش اینترنتی مسئله امنیت نه تنها برای شرکتها وبانکها بلکه برای عموم افراد مهم شده است.

واژگان کلیدی: امنیت، بیومتریک، بانکداری.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۸، زمستان ۱۳۹۶، ص ۱۲۹- ۱۱۸

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

خطوطی که بر روی سرانگشتان همه انسانها نقش بسته از دیر باز مورد توجه همه بوده است،این خطوط نقشهای مختلفی دارند،یکی از این وظایف ایجاد اصطکاک بین سر انگشتان و اشیاء متفاوت است مانند قلم که با استفاده از این اصطکاک می توانیم اشیاء را برداریم ،بنویسیم،یا لمس کنیم.از سوی دیگر این خطوط برای هر شخص منحصر به فرد است ،از سالها پیش از اثر انگشت افراد در جرم شناسی استفاده می شود،و امروزه در علم بیومتریک نیز از آن استفاده می شود. مانند تمام دیگر اعضاء بدن DNA های هر شخصی الگوی ساخت این خطوط را دارا هستند و در واقع DNA های هرشخص نیز کاملا منحصر به فردند و این قضیه تقریبا در مورد تمام دیگر اعضاء بدن صادق اند. با وجود hacker ها و دزدی های اینترنتی Password ها ابزار قابل اعتمادی نیستند.بیومتریک علم شناسایی افراد از طریق مشخصات انسانی اوست که شامل اثر انگشت،کف دست ،صورت ، امضاء ، دست خط ،اسکن عنبیه و شبکیه ، صدا است. در علم بیومتریک اعضایی از بدن مورد توجه قرار گرفته که استفاده از آنها راحتتر و کم ضرر تر باشد. هر کدام از روشهای مورد استفاده دارای نقاط ضعف و قدرتی هستند که با ترکیب آنها با دیگر روشهای امنیتی می توان ضعفهای موجود را از بین برد.

هیچ فردی نمی خواهد هنگام چک کردن موجودی خود از طریق شبکه های online بانکها متوجه شود که مو جودیش خالی شده ، در بسیاری از موارد به علت معنی دار بو دن Passwordها افرادی که تا حدی ما را می شناسند میتوانند آنها را حدس بزنند و با فهمیدن شماره ما در بانک به راحتی با استفاده از شبکه onlineبانک وارد حساب ما شده موجودی ما را خالی کنند.با توجه به سرعت رشد قابل توجه تجارت جهانی و اهمیت تجارت نمی توان از سیستمهای قدیمی دستی یا حضوری برای مدت زمان طولانی استفاده کرد، از طرف دیگر استفاده از این روشهای قدیمی با عث اتلاف انرژی و زمان زیاد شده و در مدت زمان طولانی کار کمتری انجام می شود. بنابرین در تجارت ، به موضوع تجارت الکترونیکی نیاز احساس می شود و موضوع بسیار مهمی که امروزه مورد توجه است مسئله امنیت وsecurityاست. Biometric با استفاده از روشهای قابل اعتماد میتواند تا حد زیادی جوابگوی مشکلا تی از این قبیل باشد. علمBiometric نه تنها در مورد تجارت الکترونیک بلکه در موارد بسیار دیگری نیز کاربرد دارد. به عنوان مثال در آزمایشگاهای مهم و حساس یا ورودیها ی ساختمانهایی که در مورد ورود و خروج از آنها حساسیم یا می توانیم از قفلهایی که روی آنها صفحه کلید نصب شده استفاده کنیم و به افراد مورد نظر اسم رمز عبور بدهیم تا هنگام ورود از آن استفاده کرده داخل شوند ولی این روش نیز زیاد قابل اعتماد نیست با لو رفتن کلمه عبور دیگر این کار به درد نخور خواهد شد. ولی زمانیکه از اثر انگشت یا کف دست یا ... برای شناسایی و اجازه ورود استفاده شود دیگر این مسائل ایجاد نخواهد شد. بعد از شرح اهمیت این موضوع به بررسی Biometric می پردازیم.در تمام مواردی که ذکر خواهد شد ابتدا با استفاده از وسایل مخصوص آن روش معمولا تا ۳ بار الگوی اولیه گرفته می شود و بعد از بدست آوردن بهترین الگو ، ذخیره می شود و موقع شناسایی با این الگو مقایسه انجام می گیرد.در Biometric از مشخصا ت فیزیکی و رفتاری برای شناسایی افراد استفاده میشود، مشخصات فیزیکی مانند:اثر انگشت، اسکن دست ، صورت وچشم که خود به دو دسته اسکن عنبیه و شبکیه تقسیم می شود. مشخصات رفتاری مانند:صدا، امضاء، تایپ.

۱-بیومتریک، آینده بانکداری مجازی

آینده بانکداری مجازی را باید در سیستم های احراز هویت کاربران شبکه های بانکی دانست. افزایش کلاهبرداری اینترنتی و توسعه جرایم سایبر (Cyber crime)، از جمله مواردی هست که سبب می شود تا بانکداری مجازی را به سمت و سوی افق های نوین در استقرار نظام بانکداری الکترونیک کم خطر، سوق دهد(۱).

۱-۱ بیومتریک چیست؟

زیست سنجشی یا بیومتریک به نوع خاصی از روش‌های امنیتی گفته می‌شود که در آن برای کنترل دسترسی و برقراری امنیت از خواص قابل اندازه‌گیری بدن انسان یا هر موجود زنده دیگر استفاده می‌شود، همانگونه که از کلمه بیومتریک بر می‌آید در این روش با استفاده از الگوریتم‌های ریاضی از اندام‌ها برداشت‌های ثابت و یکتایی می‌شود که می‌توان از آن به عنوان یک کلمه عبور یکسان و غیر قابل تقلید و گاه غیرقابل تغییر استفاده کرد . اگرچه ممکن است این اسم به نظر غریب و جدید بیاید اما واقعیت این است که بشر مدت زیادیست که از آن بهره می‌برد و مثال زنده آن استفاده از عکس‌هایست که در کارت‌های مختلف از آن بهره می‌بریم، در واقع در تمامی آن کارت‌ها شخص کنترل کننده با دیدن عکس و مقایسه آن با چهره واقعی شما از اصول اولیه زیست‌سنجی (بیومتری) پیروی می‌کند یکی دیگر از اینگونه مثال‌ها استفاده از اثر انگشت است که قدمتی بس طولانی در بین اذهان عمومی بشر دارد . به نظر می رسد سیستم کد کاربری و رمز عبور، خیلی برای هزاره سوم میلادی، نسخه جالب و قابل اعتمادی نیست و تلاش صنعت بانکداری بر این موضوع استوار شده است که روش های خلاقانه و پر اعتمادی را در اختیار میلیاردها کاربر شبکه بانکداری الکترونیک که در حال یکپارچه سازی خدمات به

ISSN: 2745-3673
http://www.Rcsj.ir

مشتریان هست، قرار دهد. شاید، موزه ها، مراکز گردشگری و اماکنی که بازدید کننده زیادی دارند، دیگر از مشتریان خود، بلیط الکترونیکی یا چاپی قبول نکنند. از شما خواسته می شود تا بر اساس اطلاعات بیومتریکی که دارید، در پرتال مربوط به اماکن گردشگری ثبت نام کنید و سپس پس از ثبت نام، به باجه ای که مستقر در محل گردشگری خاص ثبت نام شده هست مراجعه کنید و اثر انگشت خود را ان جا وارد کنید. اکنون، اجازه عبور از گیت کنترل برای شما صادر می شود. نه کاغذی چاپ می شود، نه بلیطی صادر می شود و نه کنترل انسانی نیاز هست. از گیت، کسانی عبور می کنند که در سایت ثبت نام کرده و اطلاعات بیومتریک آن ها ثبت شده و هزینه را از طریق بانکداری اینترنتی پرداخت کرده اند.

این سیستم در صدها هزار مرکز گردشگری در دنیا می تواند استفاده شود و صرفه جویی مالی و انسانی بسیاری را سبب می شود. به هر حال، صنعت گردشگری ، نیازمند پتانسیل های جدید و خلاقانه هست تا گردشگران بتوانند با این قابلیت های فناورانه، بیش تر به سفر آسان و ایمن و راحت، ترغیب و تشویق شوند. صنعت سرویس های مالی باید برای حصول اطمینان از سازگار فناوری های بیومتریک با خدمت جدید، رقابت را کنار بگذارد و به دنبال ارائه سرویس های راحت به کاربران نهایی باشد. نشخیص هویت بیومتریکی ، مساله مهمی است که باید در نظر داشت. در حال حاضر، ۲۲ درصد از بانک های غربی، خدمات بیومتریکی را به مشتریان خود ارائه می کنند و ۶۵ درصد نیز قصد دارند این سرویس ها را در آینده نزدیک ارائه کنند. فناوری بیومتریک، به ۲ صورت انگشتی و هم چنین تشخیص صدا ارائه می شود و به نظر می رسد در این سو، نقش هوش مصنوعی و وب ۲ به عنوان ابزار توسعه بیومتریک در فناوری های نوین بانکداری مجازی، بسیار حساس باشد. به نظر می آید در آینده نزدیک، استقرار سیستم های بیومتریک در اپلیکیشن های موبال بانکینگ، با کمک غول های فناوری از جمله گوگل و اپل، گسترش یابد و گوشی های نسل جدید در چند سال آینده، ظرفیت های بیومتریک را برای ورود به سامانه های بانکداری مجازی ارائه کنند. برای کسب اطلاعات بیش تر در این عرصه، می توانید به پرتال و paymentscardsandmobile.com مراجعه کنید(۲).

۲-فناوری‌های بیومتریک در خدمت احراز هویت؛ تقابل راحتی و حریم خصوصی

مدیر اجرایی در بخش بازاریابی شرکت SapientNitro درباره هنر فناوری تشخیص هویت این‌طور می‌گوید: «سلیقه شخصی من اعمال دانش در بخش‌هایی از فناوری است که به طور سنتی در هنر به آن‌ها اشاره شده است. براس مثال، صورت؛ هر کسی یک صورت دارد، اما تفاوت‌های بسیاری وجود دارد. هر صورتی داستان متفاوتی دارد، اما صورت‌ها ویژگی‌های استانداردی دارند که قابل اندازه‌گیری و مقایسه بوده و می‌توانند در تشخیص هویت به کار گرفته شوند.»در کنفرانس اخیر بیومتریک، نمایندگانی از وزرا و پلیس کشورهای برزیل، قطر وهم‌چنین پلیس بین‌الملل و بانک‌های مهم حضور داشتند. علی رغم حضور نمایندگان مختلف، سوال اصلی در این کنفرانس تقابل بین حریم شخصی و راحتی بوده است.

اگر برایتان حفظ حریم شخصی مهم است می‌توانید از رادارها دور بمانید، اما در این صورت انجام ساده‌ترین کارها نیز برایتان مشکل خواهید بود، مانند سوار اتوبوس شدن و یا رفتن به دکتر. اما اگر برایتان راحتی مهم است و حفظ حریم شخصی زیاد برایتان اهمیت ندارد، در این صورت احتمالاً باید به دیگران اجازه دهید کنترل کارهایتان را به دست بگیرد.تشخیص هویت به خودی خود مساله دشواری نیست. DNA مجموع DNA های والدین است، اما در عین حال این ترکیب منحصر به فرد است. بافت عنبیه، اثر انگشت، و برخی دیگر از ویژگی‌های فیزیکی منحصر به فردند.

تعریف هویت امری پیچیده است، و این تعریف به این‌که کجا زندگی می‌کنید، و یا کار می‌کنید وابسته است.

برای مثال، اگر در کشوری زندگی می‌کنید که سرویس‌های شهروندی ضعیفی دارد، ثبت تولد و مرگ کار دشواری خواهد بود. در مثال رای‌گیری، تعدادی از ثبت‌نام کنندگان برای رای ممکن است تا زمان رای گیری مرده باشند. در کشورهای پیشرفته‌تر بدون داشتن یک شناسه قابل تایید، نمی‌توانید رای داده، به مدرسه رفته و یا خدمات درمانی دریافت کنید. از طرفی حقوق انسانی مساله‌ساز است.واضح است توانایی در تفاوق بین افراد مختلف از ابتدای پیدایش گونه‌های مختلف مهم بوده است. حتی لئوناردو داوینچی سعی کرده بود به این سوال پاسخ دهد چه چیزی باعث تمایز بین صورت‌های افراد مختلف می‌شود.امروزه از معیارهای بیومتریک این‌چنینی برای تمایز بین افراد استفاده می‌شود؛ به طور مثال اپل و سامسونگ با هم بیش از نیم میلیون دستگاه که پویشگر اثر انگشت دارند را روانه بازار کرده‌اند. این بدان معنا نیست که ما آن‌قدر تنبل و یا کندذهن هستیم که نمی‌توانیم یک عدد ۴ رقمی را به خاطر بسپاریم، بلکه بدان معناست که روش‌های یاد شده به آسانی توسط دیگران قابل انجام اند. اگر به دقت به زندگی دیجیتال خود بنگریم، می‌بینیم که آسیب‌پذیری مان تا حد زیادی در گرو تلفن‌های همراه است.بنابریان تشخیص هویت در زندگی‌مان اهمیت به سزایی دارد. و به همین ترتیب فناوری‌های جدید بیومتریک به ما در این عرصه کمک کرده‌اند(۳و۴).

ISSN: 2745-3673
http://www.Rcsj.ir

۳-چالش‌های احراز هویت در بانکداری الکترونیک

امنیت یکی از چالش‌های اصلی استفاده در فناوری اطلاعات در بانک‌ها است که روز به روز بر اهمیت آن افزوده می‌شود. سهل‌انگاری در مقوله امنیت می‌تواند صدمات جبران ناپذیری را بر بدنه شبکه بانکی کشور وارد کرده و این حوزه را با چالش جدی مواجه سازد. یکی از حوزه‌های امنیت که کاربرد فراوانی در بانکداری الکترونیک دارد تکنولوژی‌های احراز هویت است. از آنجا که عملیات بانکی اعم از تراکنش‌های مالی و پولی، افتتاح حساب، گزارش‌گیری از تراکنش‌ها و ... باید توسط افراد مجاز مانند صاحبان حساب‌های بانکی یا کسانی که از آن‌ها وکالت دارند یا توسط کاربران و کارمندان مجاز بانک‌ها، قابل‌انجام باشد، احراز هویت درخواست‌کننده عملیات بانکی از مسائل مهم امنیتی در حوزه بانکداری الکترونیکی است. یکی از مشکلات احراز هویت در اینترنت بانک مشهود است، امروزه سیستم بانکی با احراز هویت کاربران اینترنتی خود مشکل دارد و اطمینان از اینکه خود کاربر از اینترنت بانک استفاده کرده است کار دشواری است حتی رمزهای یکبار مصرف (OTP) هم نتوانستند این مشکل را حل کنند؛ چرا که با دسترسی به این دستگاه می‌توان بدون حضور مالک دستگاه هم از آن استفاده کرد. امروزه پویایی و امنیت یک سیستم را با احراز هویت سنجش می‌کنند و در حقیقت سیستمی که احراز هویت در آن موجود نیست، سیستم ناامنی است(۵).

در زیر روش‌های احراز هویت را بیان می‌کنیم:

احراز هویت با کلمه عبور

احراز هویت با امضا

احراز هویت با داشتن یک کارت بانکی

احراز هویت با استفاده از یک نشانه (توکن)

احراز هویت بیومتریک (اثر انگشت، عنبیه چشم و...)

احراز هویت ترکیبی (ترکیبی از موارد فوق‌الذکر)

۳-۱-تهدیدهای موجود در سیستم‌های احراز هویت:

۳-۱-۱-احراز هویت با کلمه عبور

کلمه عبور متداول‌ترین سیستم برای احراز هویت در نظام بانکداری الکترونیک است با این حال سیستم قابل‌اطمینانی برای تشخیص احراز هویت نیست به دلیل اینکه اطمینان از اینکه خود شخص از کلمه عبور استفاده کرده کار دشواری است به همین دلیل برای داشتن سیستم کاملاً امن نمی‌توان به این سیستم اتکا کرد.

۳-۱-۲-احراز هویت با امضا

یکی از ابتدایی‌ترین روش‌های احراز هویت است. به این صورت که امضای کاربر با امضای ثبت شده در سیستم بانکی مطابقت داده می‌شود، ولی این روش هم نمی‌تواند سیستم امنی باشد که بتوان از آن به‌صورت گسترده استفاده کرد. عواملی چون خطای انسانی و جعل، امنیت این روش را زیر سوال می‌برد.

۳-۱-۳-احراز هویت با استفاده از توکن

استفاده از توکن به معنی استفاده از موجودیت‌ها است که این موجودیت‌ها می‌تواند کارت شناسایی، کارت بانکی، اسمارت کارت و... باشد که متناسب با محیط مورد استفاده قرار می‌گیرد. با این روش هم نمی‌توان هویت فرد را تشخیص داد به دلیل اینکه ممکن است توسط فرد دیگری مورد استفاده قرار گیرد و مشکلاتی همچون مفقود شدن، جعل و... نیز برای این موجودیت‌ها اتفاق بیفتد و در پاره‌ای مواقع برای احراز هویت نیاز به ارائه چند موجودیت است به همین دلیل نمی‌توان از آن در حجم وسیع استفاده کرد(۶).

۳-۱-۴-احراز هویت با استفاده از بیومتریک

در این سیستم از خصوصیت‌های فیزولوژیک بدن انسان استفاده می‌شود. این خصوصیت‌ها می‌تواند اثر انگشت، عنبیه چشم، صدا، چهره و... باشد. استفاده از این روش بنا به خصیصه مورد استفاده مشکلات خاص خودش را دارد. متغیرهای بیومتریک باید این ویژگی‌ها را داشته باشند:

همه افراد آن را داشته باشند

ISSN: 2745-3673
http://www.Rcsj.ir

این خصیصه باید متمایز باشد و در هیچ دو نفری یکسان نباشد که در خصیصه‌هایی که در بالا از آن‌ها نام بردیم این ویژگی موجود است ؛ در طول عمر افراد تغییر نکند.

۳-۱-۵-احراز هویت با استفاده از سیستم‌های ترکیبی

این روش تشکیل شده از روش‌های احراز هویتی که در متن فوق از آن‌ها صحبت کردیم که این روش می‌تواند ترکیب احراز هویت با کلمه عبور و احراز هویت با توکن‌ها باشد یا ترکیب احراز هویت با توکن و متغیرهای بیومتریک یا غیره باشد. این روش از امن‌ترین روش‌های احراز هویت است؛ چون از دو روش به‌طور همزمان استفاده می‌شود. در این روش ممکن است از احراز هویت با کارت بانکی و کلمه عبور هم‌زمان با هم استفاده شود که در این صورت هم نمی‌توان گفت این روش کاملاً امن است. از روش‌های ترکیبی دیگر می‌توان به استفاده از رمزهای یکبار مصرف که توسط دستگاه‌های رمزیاب تولید می‌شود و رمز ثابت فرد اشاره کرد. رمز یکبار مصرف توسط دستگاه رمزیاب تولید می‌شود، دستگاه رمزیاب یک دستگاه فیزیکی است که در اختیار کاربر قرار می‌گیرد و با تولید یک عدد یکتا به‌صورت تصادفی و از روی سرور، احراز هویت کاربری که آن را وارد کرده است، تایید می‌کند؛ اما در دستگاه‌های رمزیاب هم مشکلاتی نظیر تمام شدن باتری یا به سرقت رفتن و... وجود دارد که استفاده از این دستگاه را دچار مشکل می‌کند.

برای مقابله با این مشکلات چه می‌توان کرد؟ پیشنهاد ما استفاده از یک راهکار خلاقانه و نوین است. این راهکار در واقع یک سلاح موثر در مقابل تمامی تهدیدهای فوق است که به آن اشاره کردیم و به تولیدکنندگان این سیستم‌ها امکان انجام احراز هویت ایمن برای کاربردهای آنلاین را می‌دهد. راهکار ما استفاده از سیستم ترکیبی است اما سیستمی که در آن حضور شخص یک امر ضروری برای احراز هویت است. این راهکار ترکیب احراز هویت به‌صورت بیومتریک و یک اسمارت کارت است که در زیر بیشتر در مورد این روش توضیح می‌دهیم(۷).

۳-۱-۶-احراز هویت با اثر انگشت و اسمارت کارت

این سیستم شامل یک اثر انگشت اسکنر و اسمارت‌کارت‌خوان است که به این تکنولوژی Match On Card می‌گویند. این سیستم احراز هویت دارنده کارت را بدون نیاز به شبکه به‌صورت آفلاین انجام می‌دهد. این سیستم اطلاعات شخص نظیر نام و نام خانوادگی، عکس و... و اطلاعات بیومتریک را که در اینجا همان اثر انگشت کاربر است، به واسطه امنیت کارت هوشمند روی Chip کارت ذخیره می‌کند. ذخیره‌سازی اثر انگشت برای هر ۱۰ انگشت دست صورت می‌گیرد که این ذخیره‌سازی به شکل عکس نیست و با استفاده از الگوریتم رمز شده اثر انگشت صورت می‌گیرد که همین امر ضامن امنیت این روش است. از مزیت‌های این روش این است که شخص نمی‌تواند هویت خود را انکار کند چون در زمان استفاده باید خود شخص به‌صورت زنده و اسمارت کارت حاوی اطلاعات بیومتریک و اطلاعات شخصی وجود داشته باشد و از دیگر مزیت‌های این دستگاه می‌توان به رمزنگاری و رمزگشایی اطلاعات اشاره کرد(۸).

۳-۱-۷-قابلیت‌های این روش

استفاده از این روش ممکن است بعد از احراز هویت منجر به ایجاد یک رمز یکبار مصرف شود.
استفاده از این روش ممکن است موجب ایجاد یک امضای دیجیتال برای اسناد باشد.
می‌توان از این روش برای ایجاد امنیت صندوق‌های امانات بانک‌ها استفاده کرد.
این روش، روشی مطمئن برای احراز هویت کاربر در استفاده از اینترنت بانک است.
استفاده به‌صورت آفلاین.

۴-بیومتریک جایگزین رمز عبور

با عرضه تلفن‌های هوشمند آیفون X10 اپل به بازار، کمتر کسی متوجه ورود بی‌سروصدای بشر به عصر بیومتریک شد. اپل با خرید شرکت AuthenTec در سال ۲۰۱۲ به این فناوری دست یافت. ازسوی‌دیگر نیز سامسونگ در اقدامی رقابتی، نسخه‌های خود را از این فناوری در گوشی‌های گلکسی S8 و گوشی‌های گوشی های نت۸ که به بازار ارائه شد، روانه بازار کرد.شرکت مخابراتی Qualcomm نیز متعهد شده است به‌زودی حسگرهای سه‌بُعدی اثرانگشت را در محصولات خود تعبیه کند. با این روند، به‌نظر می‌رسد این فناوری در گوشی‌های هوشمند، در دو سال آینده، به‌طور فزاینده‌ای استانداردتر شود.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۸، زمستان ۱۳۹۶، ص ۱۲۹- ۱۱۸

ISSN: 2745-3673
http://www.Rcsj.ir

بانک‌های RBS و NatWest به‌تازگی اعلام کرده‌اند مشتریانشان به‌زودی می‌توانند از طریق Touch ID(احراز هویت از طریق لمس اثرانگشت) کارهای بانکی خود را انجام دهند. اما «جان کریسلر»، هکر آلمانی با نام مستعار «استارباگ» تسلیم این فناوری‌ها نشده است. او فقط چندروز پس از عرضه اپل به بازار، Touch ID آن را هک کرد و این کار را فقط با استفاده از کیتی که شامل یک اسکنر، یک پرینتر و اندکی چسب و اسکن تکرار آخرین اثر انگشتی که صفحه شیشه‌ای آیفون را لمس کرده بود، انجام داد. او سپس در ماه سپتامبر با استفاده از عکس‌های وزیر دفاع آلمان که در یک نشست خبری از فاصله سه متری گرفته شده بود، اثر انگشت این وزیر را بازآفرینی کرد. استارباگ معتقد است حفاظت مناسب، نیازمند یک احراز هویت دوعاملی است که براساس دو مؤلفه کاملا مستقل از یکی از سه روش: رمز عبور- اطلاعاتی، کارت‌های هوشمند شخصی و ویژگی‌های بیومتریک تعریف شده باشد.

این امنیت بر پایه آن اطلاعاتی که می‌دانید آنچه دارید و آنچه هستید، برقرار می‌شود. این هکر می‌گوید: دو روش از این سه روش می‌توانند یکدیگر را همپوشانی کنند، به‌طوری‌که می‌توان اطلاعات محرمانه یک روش روی دستگاه را از طریق روش دوم کشف کرد؛ مثلا اگر بتوانید از روی اثر انگشتی که روی تلفن جا مانده، یک انگشت جعلی بسازید این دو عامل در واقع به اندازه یک عامل ارزش دارند. آسیب‌پذیری در تشخیص اثر انگشت، موضوع محرمانه‌ای نیست و همین امر، موجب شده محققان به تلاش و رقابت برای یافتن یک جایگزین بیومتریک برای آن ادامه دهند. این امر با حسگرهایی که به‌وفور و ارزان تولید می‌شوند، تسریع شده است و اغلب، شاهد تولید نرم‌افزارهایی هستیم که شرکت‌های جنوب‌شرق آسیا با تکیه بر فناوری خدمات ابری عرضه می‌کنند. بارکلی، امسال احراز هویت رگ انگشت دست را برای مشتریان انگلیسی خود ارائه می‌کند. این فناوری را شرکت ژاپنی هیتاچی تولید کرده و در دستگاه‌های خودپرداز ژاپن و لهستان از آن استفاده می‌شود.

متخصصان هیتاچی می‌گویند الگوی عروق در زمان جنینی شکل می‌گیرد و در سراسر عمر، ثابت می‌ماند. وقتی نور فروسرخ از انگشت می‌گذرد، بخشی از آن جذب هموگلوبین رگ‌ها می‌شود. ازاین‌رو اسکنر احراز هویت رگ هیتاچی می‌تواند هویت فرد را از طریق بررسی الگوی رگ تصدیق کند.«استالر» استارت‌آپ انگلیسی با هیتاچی و BT روی راهکار پرداخت با اثر انگشت کار می‌کند و این کار را در چندین جشنواره موسیقی آزمایش کرده است. آنها نام این نوع پرداخت را «پرداخت انگشتی» (FingoPay) گذاشته‌اند. در این روش، کاربر انگشت را روی اسکنر قرار داده و چند رقم آخر کارت اعتباری خود را به فروشنده می‌گوید و به‌همین‌سادگی پرداخت به صورت زمان واقعی انجام می‌شود. روش‌های بیومتریک بسیار متنوعی به بازار عرضه شده‌اند که ازآن‌جمله می‌توان به Nymi اشاره کرد. این فناوری که توسط شرکت کانادایی «بیونیم» عرضه شده، دستبندی است که هویت کاربر را بر اساس پالس‌های الکتریکی ضربان قلب که کاملا منحصربه‌فرد است- تعیین می‌کند(۹).

شرکت آلمانی Cognitec نیز پس از تمرکز اولیه بر فناوری اثر انگشت، اکنون روی تشخیص چهره کار می‌کند. مقامات این شرکت می‌گویند دراین‌زمینه قراردادی را با پلیس مرزی آلمان منعقد کرده‌اند. شرکت آمریکایی EyeLock در حال تولید اسکنرهای تجاری عنبیه موسوم به Myris است. این شرکت مدعی است که فقط «دی‌ان‌ای» احراز هویت دقیق‌تری از فرد ارائه می‌دهد. اما آنهایی که در زمینه فناوری‌های مالی کار می‌کنند معتقدند استفاده از چندین مورد از این اسکنرهای بیومتریک برای بانک‌ها و شرکت‌های اعتباری که قصد معرفی خودشان به مشتریان معمولی را دارند، مشکل‌زاست. دکتر «نیل کاستیگان»، رمزنگار ایرلندی و مدیرعامل شرکت سوئدی BehavioSec بر این باور است برای این شرکت‌ها بخش گران‌قیمت و دردسرساز درواقع به‌چالش‌کشیدن کاربر یا همان مشتری است.

به گفته او، پرسیدن یک‌سری سؤالات، ازجمله «اسم حیوان خانگی» یا «ماشین‌حساب را کجا می‌گذارید» برای کاربر اذیت‌کننده است. با هرگام از امنیت که از کاربر می‌خواهد کاری انجام دهد درواقع از تعداد پرداخت‌ها کم می‌شود. برخی از شرکت‌های فناورانه نیز روی تشخیص صدا برای احراز هویت‌های بانکی کار می‌کنند؛ چراکه خیلی برای مشتریان دردسرساز و دشوار نیست. گروهی از محققان نیز در تلاش برای کاشت ایمپلنت‌های بیومتریک هستند؛ مانند تراشه احراز هویت فرکانس رادیویی که زیر پوست کار گذاشته می‌شود یا خالکوبی‌های پاک‌شدنی که بتواند یک یا دو ماه دوام بیاورد. دولت‌ها و مؤسسات خصوصی بیشتر ترجیح می‌دهند از نظر امنیت زیاد سخت نگیرند و مشتریانشان را نیازارند.

یک جایگزین دیگر برای احراز هویت، بیومتریک رفتاری است؛ یعنی بررسی ژست و سرعتی که کاربر رمزعبور خود را به سیستم وارد می‌کند. وقتی Danske Bank تلاش داشت تایمری را به پلت‌فرم بانکداری الکترونیک خود معرفی کند، دریافت سرعتی که کاربر فرم آنلاین را پر می‌کند، می‌تواند در ۹۷/۴ درصد موارد یک کاربر واقعی را از یک متقلب مشخص کند. پیش‌بینی بسیاری از کارشناسان این است که بیومتریک، مرگ رمز عبور را رقم خواهد زد. برخی از کارشناسان بر این باورند ابزارهایی مانند کلید امنیتی فیزیکی HSBC و کارت‌های اعتباری دیگر پایشان لب گور است.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۸، زمستان ۱۳۹۶، ص ۱۲۹- ۱۱۸

ISSN: 2745-3673
http://www.Rcsj.ir

۵-بازار پر رشد فناوری‌های احراز هویت

نگرانی کاربران از افشای اطلاعات خصوصی و مالی از یک سو و افزایش قدرت هکرها در دسترسی به اطلاعات محرمانه، سبب شده بازار فناوری‌های احراز هویت کاربران بسیار داغ باشد. در این میان، فناوری‌های تعیین هویت بیومتریک برای گوشی‌های هوشمند را می‌توان پیشتاز دانست.بر اساس پیش‌بینی کارشناسان، حجم این بازار از ۱۴,۲ میلیارد دلار در سال ۲۰۱۶ به بیش از ۶۶۵ میلیارد دلار در سال ۲۰۲۱ خواهد رسید. به همین دلیل می‌توان پیش‌بینی کرد در چند سال آینده، فناوری‌هایی پیشرفته‌تر برای افزایش هرچه بیشتر امنیت در تعیین هویت به بازار وارد شوند.

۵-۱-فناوری بیومتریک و نقش آن در زندگی

پیدایش رایانه در صحنه زندگی بشر تحولات بزرگی را به وجود آورد که استفاده از فناوری های جدید مانند هوش مصنوعی وفناوری بیومتریک را باید عرصه پهناور تلاقی و ملاقات بسیاری از دانش ها, علوم و فنون قدیم و جدید در دنیای رایانه دانستپیدایش رایانه در صحنه زندگی بشر تحولات بزرگی را به وجود آورد که استفاده از فناوری های جدید مانند هوش مصنوعی وفناوری بیومتریک را باید عرصه پهناور تلاقی و ملاقات بسیاری از دانش ها، علوم و فنون قدیم و جدید در دنیای رایانه دانست.فناوری جدیدی که گوی رقابت را از دیگر فناوری ها ربوده است، فناوری بیومتریک است. این فناوری برای اثبات و یا تایید هویت افراد و نیز کنترل اشخاصی که می خواهند به داده های خاصی دسترسی پیدا کنند، استفاده می شود.

۶- نوآوری

۶-۱-آیا در آینده دستگاه های خود پرداز به سیستم های شناسایی مشتری بیومتریک مجهز خواهند شد؟

مسئله دستگاه های کارتخوان، یکی از مخاطرات اصلی بانک ها و موسسات مالی محسوب می شود. انتظار می رفت عرضه کارت های هوشمند با تراشه های تعبیه شده در آن ها، روشی ایمن تر برای حفاظت از اطلاعات باشد؛ اما از آن جا که در بسیاری از موارد کارت ها دارای خطوط مغناطیسی هستند؛ در مکان هایی که نیاز به تراشه های هوشمند نیست امکان سرقت اطلاعات توسط باندهای خلافکار از طریق همین خطوط مغناطیسی وجود دارد. نیازی که در این میان احساس می شود تجهیز دستگاه های خود پرداز به سیستم های شناسایی مشتری بیومتریک است.

۶-۱-۱سیستم های شناسایی مشتری بیومتریک

راهکار سیستم های شناسایی مشتری بیومتریک سطح امنیتی دیگری در اختیار ما قرار می دهد که کپی کردن و سرقت اطلاعات از آن ممکن نیست و از خطری که بانک ها به صورت بالقوه با آن روبه رو هستند می کاهد. سامانه های شناسایی مشتری بیومتریک تا کنون در کارت های شناسایی در عبور از مرز ها و در زمینه مدیریت نیرو کار (مثلا در کنترل دسترسی و زمان حضور کارکنان) به کار گرفته شده، اما تنها این اواخر به عنوان راه حلی موثر در مورد دستگاه های خود پرداز مطرح گردیده است.

محمد مراد، معاونت فروش جهانی و توسعه تجارت جهانی شرکت آیریس آی.دی می گیود: " شناسایی از طریق چشم، به سبب سرعت و دقت آن همواره روشی مناسب برای تعیین هویت بوده است. با این حال، همیشه مسائل اقتصادی، اندازه تجهیزات و هزینه ها مواردی بوده اند که از بکارگیری آن در دستگاه های خود پرداز جلوگیری کرده است. اما در سال های اخیر مشکلات مربوط به ساخت دستگاه از نظر تکنولوژیکی و اقتصادی حل شده است. ما نمونه های آزمایشی خود را در کره، خاورمیانه و جاهای دیگر به کار گرفته ایم و تا کنون پیشرفت مناسبی داشته ایم.مراد توضیح می دهد که دستگاه های شناسایی چشمی (از طریق عنبیه) به جهت فضای کمی که اشغال می کند به خوبی قابل تعبیه در خودپرداز ها بوده و به این ترتیب، زمان تراکنش های مربوط به دستیابی به پایگاه داده و تایید هویت بسیار سریع خواهد بود. به علاوه این شناسایی به صورت گمنام خواهد بود. تصویر عنبیه به صورت یک رشته صفر و یک، ترجمه شده و با الگوهای مشابه ذخیره شده در پایگاه داده مقایسه می شود. تا آن جا که به ساختار مربوط است، شناسایی هویت از طریق چشم را می توان به چندین شیوه انجام داد؛ برای اینکار می توان از یک پایگاه داده مرکزی یا از گواهینامه های ذخیره شده بر روی تلفن یا کارت هوشمند افراد استفاده کرد (به کمک سیستم ان.اف.سی گوشی ها).

سیستم های شناسایی مشتری بیومتریک احتمالا به حذف استفاده از کارت ها منجر نخواهد شد. استاندارد سازی استفاده از روش های بیومتریک در بانک ها بسیار پیچیده و زمان بر خواهد بود و به نظر می رسد که افراد در بانک خودشان از روش های بیومتریک استفاده کنند اما احتمالا برای دسترسی به خود پرداز های خارج از شبکه بانکی خود همچنان از پین کد و کارت استفاده خواهند کرد.هنوز راه

ISSN: 2745-3673
http://www.Rcsj.ir

زیادی تا کاربرد وسیع روش های بیومتریک در خود پردازها باقی مانده است، اما نمونه های آزمایشی شرکت ها به تدریج این مسئله به واقعیت تبدیل خواهند کرد.به گفته آقای مراد موسسات مالی بسیار محافظه کار هستند و تغییر تکنولوژیکی در آن ها سهل و ساده نیست. در نتیجه پیشرفت کار کند است اما نشانه های مثبتی دیده می شود. در ابتدای کار بیشتر موسسات مالی از شناسه گر بیومتریک همراه با کارت های خود پرداز شماره رمز برای دسترسی به تراکنش های مالی استفاده خواهند کرد. اما با گذشت زمان، روش های بیومتریک، مانند روش مبتنی بر شناسایی عنبیه چشم، احتمالا نیاز به رمز را از بین خواهد برد(۱۰).

۶-۱-۲-چشم انداز

کارت های بانکی برای امنیت بیشتر از خطوط مغناطیسی به تراشه ها متوسل شدند و احتمالا در مرحله بعد به سمت شناسایی از طریق عنبیه چشم یا اثر انگشت افراد خواهند رفت. استفاده از روش های شناسایی بیومتریک در خود پرداز ها، دورنمایی جالب برای غلبه بر مشکلاتی مثل کلاه برداری و خوانش کارت ها توسط دیگران است. روش های بیومتریک می توانند امکان شناسایی چند عاملی را فراهم کرده، سطح امنیتی را بالا برده و خطر سرقت هویت را به میزان زیادی کاهش دهند. اما این تنها یک قدم در رقابت همیشگی میان بانک ها و تبهکاران است و تبهکاران بدون شک تلاش می کنند راهی برای غلبه بر این مشکل پیدا کنند. مشاهد و بررسی راه حل هایی که صنعت بانکداری در آینده اتخاذ خواهد کرد قطعا جالب خواهد بود.

۶-۲-استفاده از سلفی برای احراز هویت و خرید آنلاین

طبق گزارشی که سونی موبایل و شرکت فیوچریزون انجام داده‌اند، به دلیل اینکه انداختن عکس‌های سلفی در بین افراد محبوبیت بسیاری دارد، در آینده نزدیک می‌توان از این عکس‌ها در حوزه بانکداری آنلاین، ویزیت پزشک و موارد دیگری استفاده کرد.به گزارش خبرگزاری مهر به نقل از دیلی میل، بر اساس تحقیق انجام شده هر فرد به‌طور متوسط ماهانه ۲۴ عکس سلفی می‌گیرد. بر همین اساس طی پنج سال آتی فناوری‌های مختلفی برای به کار گرفتن سلفی‌ها به بازار می‌آید. طبق این تحقیق می‌توان از عکس سلفی به‌عنوان راهی برای احراز هویت در حساب‌های مختلف بانکی و انجام پرداخت آنلاین استفاده کرد.دکتریان پیرسون دراین‌باره می‌گوید: «تحقیق ما نشان داده است افراد نسبت به کاربردهای آتی از عکس‌های سلفی بسیار خوش‌بین هستند.»به گفته پیرسون علاوه بر استفاده از سلفی در بانکداری آنلاین، راهی برای خرید آنلاین نیز به حساب می‌آید.کاربر می‌تواند با گرفتن یک سلفی تمام‌قد از خود لباس‌های مختلف را برای خود اندازه‌گیری کند و بدون خروج از خانه، خرید خود را انجام دهد(۱۱).

۷-کارهای انجام شده

۷-۱- JCB احراز هویت بیومتریک جدیدی را برای پرداخت‌های بدون کارت آزمایش می‌کند

شرکت ارائه‌کننده خدمات پرداخت‌کارتی ژاپن JCB تکنولوژی احراز هویت اسکن رگ‌های زیر پوست شرکت Fujitsu را برای پرداخت‌های بدون کارت در پایانه‌های فروش و خودپردازها آزمایش می‌کند. در ماه جولای، شرکت JCB اثربخشی سیستم احراز هویت جدید را بر روی صدها تن از کارمندان خودش آزمایش می‌کند. کارمندان JCB از این تکنولوژی برای پرداخت هزینه خرید مواد غذایی و نوشیدنی‌های موردنظر خود در کافه‌تریای دفاتر شرکت JCB استفاده می‌کنند.داده‌های حاصل از تصویربرداری رگ‌های کف دست مشتریان، به همراه اطلاعات کارت‌های پرداختی در دیتاسنترهای شرکت فوجیتسو ذخیره می‌شود. بنابراین مشتریان هنگام پرداخت هزینه‌های خود، کافی است دست خود را مقابل سنسور تکان دهند. از سرورهای احراز هویت بر اساس کف دست، اطلاعات کارت پرداخت خوانده می‌شود و فرایند تراکنش تائید می‌گردد. با توجه به تعداد افرادی که برای عضویت ثبت‌نام کرده‌اند، ممکن است به یک کلید چندرقمی برای واردکردن رمز نیز نیاز باشد تا فرایند احراز هویت تسریع شود.

تاک واتانابه، مدیر بخش زیرساخت و تکنولوژی JCB می‌گوید: « ما در حال حاضر این تکنولوژی را برای جوامع جهانی متفاوت آزمایش می‌کنیم و قصد داریم برنامه‌ای برمبنای بیومتریک های منحصربه‌فرد و با استفاده از احراز هویت امن الگوی رگ‌های کف دست توسعه دهیم. من مطمئن هستم این روش پرداخت جدید که بر مبنای تکنولوژی نوآورانه طراحی شده است، در راستای پاسخگویی به نیازهای کلیه مشتریان و شرکای JCB در سراسر جهان ارائه می‌شود.»

فوجیتسو اعلام کرده است؛ درمجموع ۴۷۰ هزار دستگاه احراز هویت را آماده کار ساخته‌اند و این تعداد برای ۶۳ میلیون کاربر در حدود ۶۰ کشور دنیا قابل‌استفاده است. پژوهش‌های اخیر که توسط شرکت مشاوره Technavio صورت گرفته است، نشان می‌دهد؛ جامعه احراز هویت بر اساس شاخص‌های بیومتریک در صنعت بانکداری، سرویس‌های مالی و بخش بیمه (BFSI)، در سال‌های ۲۰۱۶-۲۰۲۰ با

ISSN: 2745-3673
http://www.Rcsj.ir

نرخ رشد سالانه ۲۷,۸۳ درصد پیشرفت می‌کند.این شرکت در گزارش‌های خود آورده است:«تشخیص هویت بیومتریک بر اساس الگوی رگ‌ها اهمیت قابل‌توجهی در بخش BFSI و اپلیکیشن های کنترل دسترسی منطقی و کنترل دسترسی فیزیکی، بانکداری موبایلی، بانکداری در شعبه‌ها، کیوسک‌ها، دستگاه‌های خودپرداز و مسدودکننده‌های حساب‌های بانکی دارند.

۷-۲- استفاده از دو روش بیومتریک؛ راه حل امن هویت سنجی در گجت های هوشمند

محققان معتقدند که استفاده‌ی هم‌زمان از دو روش بیومتریک برای هویت سنجی در گجت‌های هوشمند، راه‌حلی برای مشکل تشخیص کاربر به‌صورت امن و سریع است. این روزها شاهد استفاده از انواع روش‌های بیومتریک برای هویت سنجی کاربران در گجت‌های هوشمند هستیم؛ ولی مشکل اصلی زمانی ایجاد می‌شود که روش هویت سنجی بیومتریک مورد استفاده قادر به شناسایی کاربر نیست و از این‌رو باید به روش‌های قدیمی با امنیت پایین دل بست. برای مثال زمانی که کاربر از هویت سنجی به روش تشخیص عنبیه استفاده می‌کند، در صورت شناسایی نشدن، کاربر باید از روش وارد کردن پین استفاده کند؛ چراکه راهکار دیگری برای ورود به سیستم وجود ندارد.برخی از کارشناسان در حال کار روی روشی هستند که در آن از دو روش هویت سنجی به‌صورت هم‌زمان استفاده می‌شود. استفاده‌ی هم‌زمان از دو روش بیومتریک از این نظر مهم است که در صورت هم‌زمان نبودن، به دلیل طولانی شدن فرایند ورود به سیستم، کاربر تمایل کمتری به استفاده از آن خواهد داشت، اما در صورت هم‌زمان بودن، علاوه بر حل مشکل عدم کارایی یک روش، دیگر نیازی به بازگشت به روش‌های گذشته نیست و ضمنا امنیت کاربر نیز با استانداردهای بهتری رعایت می‌شود. کمپانی Sensory در حال کار روی این موضوع است و تا به امروز روش‌های بسیار جالب توجهی نیز توسعه داده است(۱۲).

سنسوری به این نتیجه رسیده است که ترجیح یک روش هویت سنجی بیومتریک بر روش دیگر می‌تواند مشکلات را بیش از پیش افزایش دهد. البته زمانی که دو روش هویت سنجی استفاده می‌کنید، به مشکل برخوردن هر یک از آن‌ها باعث عملکرد نادرست سیستم می‌شود و از این‌رو بسیاری از کاربران را نیز از به‌کارگیری چنین روش‌هایی فراری می‌دهد.همان‌طور که اشاره کردیم، به‌کارگیری دو روش نیز می‌تواند در برخی سناریوها ناموفق باشد. البته استفاده از روش شناسایی صدا و چهره را باید جزو بهترین ترکیب‌ها خواند. شناسایی صدای کاربر در محیط‌های شلوغ و پر همهمه مشکل است و از سوی دیگر، شناسایی چهره می‌تواند به‌موجب تاریک بودن محیطی که کاربر در آن قرار دارد با مشکل همراه شود. از دیگر چالش‌های موجود برای این روش‌ها، تغییر آرایش چهره یا استفاده از زیورآلات و ابزارهایی نظیر عینک است که نتیجه‌ی آن به مشکل برخوردن سیستم است.

کمپانی سنسوری برای حل این مشکل، تنظیمات مربوط به هویت سنجی را متغیر در نظر گرفته است. در روش سنسوری هویت سنجی از دو طریق صوت و شناسایی چهره امکان‌پذیر است؛ با این تفاوت که هر یک از این روش‌ها به‌عنوان پشتیبانی برای روش دیگر در نظر گرفته می‌شود. در صورتی که یکی از روش‌ها در هویت سنجی ناموفق باشد، دیگری اجازه‌ی دسترسی را صادر می‌کند. در حالت نظری این روش با مشکلی روبه‌رو نخواهد شد؛ مگر اینکه کاربر برحسب اتفاق در یک مکان شلوغ و پر سروصدا و همچنین کم‌نور باشد. هرچند این موقعیت محال نیست؛ اما بسیار سخت است که چنین مشکلی گریبان‌گیر کاربر شود.قرار گرفتن در موقعیتی که اشاره کردیم بسیار نادر است؛ اما سنسوری پیشنهاد می‌دهد تا سطح سختی هویت سنجی و دقت شناسایی متغیر باشد. برای مثال دقت و ریزبینی هویت سنجی بنا بر کاری که کاربر در پی آن است، متغیر خواهد بود. برای مثال استفاده از سرویس‌های بانکی نظیر ارسال پول باید با سطح امنیتی بالاتری انجام پذیرد؛ حال آنکه اطلاع از موجودی می‌تواند با سطح امنیتی نسبتا پایین‌تری نیز انجام شود. حتی می‌توان سطح هویت سنجی را در امور بانکی بنا بر مبلغ انتقالی سخت‌تر کرد.

۷-۳- کمپانیِ سنسوری، روش ترکیبی بیومتریک برای تشخیص هویت را امن و سریع می‌داند

جنبه‌ی مثبت دیگر استفاده از دو روش بیومتریک، مقابله کارآمدتر با گمراه کردن این دو روش بیومتریک هویت سنجی است. برای مثال در صورتی که گمراه کردن شناسایی چهره را با ویدیو و صوت را صدای ضبط‌شده ممکن بدانیم، گمراه کردن هر دو روش به‌صورت هم‌زمان بسیار دشوارتر می‌شود.در واقع ترکیب دو روش بیومتریک پروژه‌ای است که سنسوری در حال توسعه و بهبود آن به‌منظور استفاده‌ی هرچه هوشمندانه‌تر است. بنا بر اظهارات گوردون هاپ، مدیر ارشد فناوری‌های دیداری سنسوری، تیم تحت مدیریت وی در حال کار برای برقراری ارتباط بیشتر بین دو روش بیومتریک شناسایی چهره و صوت است. سنسوری در نظر دارد ارتباط این دو روش را به نحوی افزایش دهد که سیستم قادر باشد با ترکیب تغییر حالت لب و صدای شنیده‌شده، صحت کلمات اداشده توسط کاربر را تشخیص دهد.با استفاده از این روش، گمراه کردن سیستم بسیار سخت‌تر خواهد شد و ادای لغاتی که به‌عنوان رمز عبور تعیین شده‌اند، برای کاربران مختلف متفاوت خواهد بود؛ چرا که صدا و حرکات لب در افراد مختلف برای ادای یک لغت متفاوت است و الگوریتم‌ها قادرند این موضوع را تشخیص

ISSN: 2745-3673
http://www.Rcsj.ir

دهند.حتی می‌توان از این روش شناسایی در دستگاه‌های خودپرداز یا ATM نیز استفاده کرد تا مانع از سرقت پول در زمان زورگیری یا تهدید کاربر به برداشت پول شد؛ چرا که لحن گفتار افراد تحت تأثیر شرایطی نظیر ترس با حالت عادی تفاوت دارد.

نظر شما در این خصوص چیست؟

۷-۴- سامسونگ احراز هویت بیومتریک را به‌صورت آزمایشی در Bank of America راه‌اندازی می‌کند

سامسونگ به‌تازگی خبر از راه‌اندازی یک برنامه آزمایشی داده است که طی آن، مشتریان Bank of America می‌توانند با عکس گرفتن از چشمانشان وارد اپلیکیشن بانکداری خود شوند.البته مشتریان این بانک از سال ۲۰۱۵ تا کنون می‌توانند با استفاده از اثر انگشت خود وارد اپلیکیشن بانکداری‌شان بشوند، اما با این حال هستند مشتریانی که هنوز با استفاده از نام کاربری و پسورد، عملیات ورود خود را انجام می‌دهند، چراکه این افراد هم افرادی سنت‌گرا هستند و هم از ترس موارد امنیتی، استفاده از روش‌های جدید را کنار گذاشته‌اند.

ویژگی اسکن عنبیه چشم، تنها بخشی از اقدامی بزرگ درجهت تغییر رفتار و برخورد به احراز هویت‌های بیومتریک است. در این برنامه آزمایشی، حدود ۱۵۰۰ کارمند شرکت سامسونگ و Bank of America، شش ماه وقت خود را صرف آزمایش و تست این تکنولوژی جدید احراز هویت می‌کنند.سامسونگ فعالیت‌هایش را در زمینه فناوری تشخیص عنبیه چشم، از ماه مارس امسال آغاز کرد و ادعایش هم این است که این تکنولوژی حتی برتر از تکنولوژی اثرانگشت FBI است. چراکه تکنولوژی اثرانگشت FBI می‌تواند ۱۳۰ شناسه منحصربه‌فرد را شناسایی کند درحالیکه این تعداد در اسکن عنبیه چشم می‌تواند به ۴۰۰ شناسه برسد(۱۳).

۷-۵- رونمایی از تکنولوژی جدید شرکت Myris برای امنیت کامپیوتر های خانگی:

محصول جدید شرکت Myris برای امنیت بیشتر کامپیوترهای خانگی رو نمایی شد. این وسیله ی کوچک امنیتی با پورت USB به کامپیوتر وصل شده و از طریق اسکن عنبیه چشم و تشخیص هویت کاربر مجوز دسترسی به کامپیوتر را صادر می کند.این تکنولوژی با استفاده از اسکن عنبیه چشم هر دو چشم را به صورت جداگانه اسکن و ۲۴۰ نقطه خاص روی هرکدام از آن ها شناسایی کرده و یک امنیت بیومتریک فوق العاده برای شما فراهم می کند.

۷-۶- رونمایی از آخرین فناوری اسکنر عنبیه چشم در MWC 2017

کمپانی آی لاک که در زمینه راهکارهای امنیتی ممتاز معروف است قصد دارد از آخرین فناوری به کار رفته در زمینه اسکنر عنبیه که مبتنی بر اسنپدراگون ۸۳۵ است، در نمایشگاه MWC 2017 رونمایی کرد. به گزارش کلیک، اسنپدراگون ۸۳۵ خود به‌تنهایی از وجود پلتفرم امنیتی موسوم به Haven بهره می‌برد که در واقع ترکیبی از سخت‌افزار و نرم‌افزار در کنار تکنولوژی‌های مرتبط با سنسورهای بیومتریک به‌منظور افزایش امنیت گجت‌های موبایل در کاربردهایی نظیر بانکداری آنلاین و همچنین پرداخت‌های اینترنتی است. پلتفرم Haven همچنین از یک راهکار شناسایی مبتنی بر سخت‌افزار بهره می‌برد که تأمین امنیت گوشی‌های هوشمند را بیش از پیش افزایش می‌دهد(۱۴).

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه‌گیری

اگرچه استفاده از شاخص بیومتریک جهت احراز هویت به صورت گسترده مراحل اولیه طفولیت خود را طی می‌کند در نتیجه استفاده از آنها در مدل‌های پرداخت به شدت محدود بوده و تجربیات بسیار اندکی پیاده‌سازی شده است تا بتواند راهگشا و هدایت‌گری برای دیگر سازمان‌ها و بانک‌ها باشد. بهره‌گیری از تکنولوژی و ترکیب آن با سیستم‌ها و نظام‌های گوناگون جدا از فرهنگ‌سازی به هنگام و غنای فنی نیازمند مجری و پیاده‌ساز متجرب دارد. تجربیات نشان می‌دهد که هنوز روش‌های بیومتریک برای شهروندان تجربه‌ای user-friend ناست. این موضوع به علت تکرر در ثبت شاخص و همچنین خطاهای هنگام خواندن، به نظر برای شهروندان چندان دلپسند نیست. از سوی دیگر وجود پایگاه‌های داده پراکنده و زیرساخت‌های کُند، باعث افزایش زمان انجام تراکنش شده است. به همین جهت در مدل پیشنهادی سامانه‌ای ملی در نظر گرفته شده است که با تجمیع ظرفیت‌ها و هزینه‌ها به صورت متمرکز بتوان زیرساختی سریع را تهیه کرد.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] K.W.Bowyer,P.J.Flynn,TheND-IRIS-0405IrisImageDataset,NotreDameCVRLTechnicalReport.(2017).
[2] J.G.Daugman,Howirisrecognitionworks,IEEETrans.CircuitsSyst.VideoTechnol.14(1)(2015)21–30.
[3] J.G.Daugman,Newmethodsinirisrecognition,IEEETrans.Syst.,Man,Cybern.B:Cybern.37(5)(2012)1167–1175.
[4] M.DeMarsico,M.Nappi,D.Riccio,ES-RU:anentropybasedruletoselectrepresentativetemplatesinfacesurveillance,MTAP,SpecialIssueonhumanvisionandinformationtheory,SpringerJ.73(1)(2014)109–128.
[5] M.DeMarsico,C.Galdi,M.Nappi,D.Riccio,FIRME:faceirisrecognitionformobileengagement,ImageVis.Comput.(2014)inpress,Availableathttp://www.sciencedirect.com/science/article/pii/S0262885614000055,doi:10.1016/j.imavis.2013.12.014.
[6] H.ElKhiyari,M.DeMarsico,A.F.Abate,H.Wechsler,Biometricinteroperabilityacrosstraining,enrollment,andtestingforfaceauthentication,in:Proceedingsof2012IEEEWorkshoponBiometricMeasurementsandSystemsforSecurityandMedicalApplications(BioMS2012),Salerno,Italy,2012,pp.1–8.
[7] B.F.Klare,M.J.Burge,J.C.Klontz,R.W.VorderBruegge,A.K.Jain,Facerecognitionperformance:roleofdemographicsinformation,IEEETrans.Inf.ForensicsSecurity7(6)(2012)1789–1801.
[8] X.Li,Z.Sun,T.Tan,Comprehensiveassessmentofirisimagequality,in:ICIP,2011.
[9] S.Marcel,etal.,Ontheresultsofthefirstmobilebiometry(MOBIO)faceandspeakerverificationevaluation,in:ICPR,2010,pp.210–225.
[10] L.Masek,P.Kovesi,MATLABSourceCodeforaBiometricIdentificationSystemBasedonIrisPatterns,TheUniversityofWesternAustralia,2003.
[11] J.R.Matey,etal.,Irisonthemove:acquisitionofimagesforirisrecognitioninlessconstrainedenvironments,Proc.IEEE94(11)(2006)1936–1947.
[12] P.J.Phillips,etal.,TheFERETevaluationmethodologyforface-recognitionalgorithms,IEEETrans.PatternAnal.Mach.Intell.22(10)(2000)1090–1104.
[13] P.J.Phillips,etal.,FRVT2006andICE2006large-scaleexperimentalresults,IEEETrans.PatternAnal.Mach.Intell.32(5)(2010)831–846.
[14] J.K.Pillai,V.M.Patel,R.Chellappa,N.K.Ratha,Secureandrobustirisrecognitionusingrandomprojectionsandsparserepresentations,IEEETrans.PatternAnal.Mach.Intell.33(9)(2011)1877–1893.