فصلنامه پژوهش در علوم، مهندسی و فناوری
دوره ۳، شماره ۴، زمستان ۱۳۹۶
صفحات ۳۳-۴۳
ISSN: 2476-5082
www.uctjournals.com

برقراری امنیت کاربران بانکی بوسیله احراز هویت بیومتریک اثر انگشت توسط رمزنگاری جریان

علی علی بابایی[۱]، دکتر علی برومندنیا[۲] و دکتر سیدجواد میرعابدینی[۳]

۱دانشجوی کارشناسی ارشد فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد الکترونیکی، گروه کامپیوتر، تهران، ایران.
۲عضو هیات علمی دانشگاه آزاد تهران جنوب، گروه کامپیوتر، تهران، ایران.
broumandnia@gmail.com
۳عضو هیات علمی دانشگاه آزاد تهران مرکزی، گروه کامپیوتر، تهران، ایران.
jvd2205@yahoo.com

چکیده

امروزه پیشرفت تکنولوژی و ارتباطات کاربرد آنها را در سیستم‌های خدمات بانکی به طور گسترده‌ای افزایش داده است. از طرفی با وجود گسترش خطرات امنیتی، نیاز به حفاظت در معاملات بانکی صدچندان احساس می‌شود. بهترین راه برقراری ایمنی در این گستره، احراز هویت کاربران در شبکه‌های گسترده‌ی بانکی است. در اینجا استفاده از داده‌های بیومتریک اثر انگشت به منظور اجتناب از استفاده‌ی یک رمز عبور در پروتکل‌های موجود پیشنهاد و پروتکلی معتبر جهت رمز کردن داده های بیومتریک طراحی شده است. جهت مقابله با تهدیدات امنیتی در سیستم‌های بانکی برخط، حفاظت از ویژگی بیومتریک اثرانگشت بوسیله پروتکل رمزنگاری جریان برقرار می‌شود. طی ذخیره‌ی داده‌های بیومتریک اثرانگشت که بسیار قابل اعتماد، در دسترس و دارای سهولت می‌باشند با الگوریتم رمزنگاری جریان، رمز شده و روش مناسب‌تری برای انجام معاملات بانکی پیشنهاد می‌شود.

واژه‌های کلیدی: احراز هویت، امنیت بانکداری، پرداخت بانکی، رمزنگاری جریان، ویژگی بیومتریک اثرانگشت.

۱. مقدمه

با گسترش فضای تبادلات و کاربردی اینترنت در بانکداری برخط[1] و سیستم‌های پرداخت الکترونیکی که بیشتر آنها از مکانیزم امنیتی نام کاربری و رمز عبور استفاده می‌کنند، خطرات امنیتی نیز افزایش یافته است. حفاظت امنیتی در تبادلات بانکی از چالش‌های بانکداری به شمار می‌رود.

برای رفع مشکل می‌توان از داده‌های بیومتریک به صورت آنی[2] در معاملات استفاده نمود. با وجود آنکه بسط و گسترش هر تکنولوژی، باعث افزایش سرعت، مدیریت زمان و مزایای دیگر است، معایبی نیز در راه دارد. استفاده از تکنولوژی بانکداری برخط، قدرت نفوذ هکرها را به همراه داشته است. چالش امنیتی احراز هویت کاربران کار دشواری شده است. برای رفع این خطرات، می‌توان در طول معامله تائید هویت بیومتریک را انجام داد. سیستم‌های بیومتریک اثر انگشت، بسیار ارزان، کاربردی و به سهولت قابل نصب و کاربر پسند است.

از طرف دیگر به لحاظ حساسیت داده‌های بیومتریک، و مقابله با سوء استفاده از آنها نیاز است به شیوه‌ی مناسبی حفاظت شوند. از بهترین راه‌های برقرای امنیت داده‌ها، رمز کردن آنهاست. پروتکل‌های رمزنگاری اجازه می‌دهد تا فرد با حساب بانکی خود ارتباط امنی را برقرار کند، امنیتی که در یک شبکه سراسری و باز صورت می‌پذیرد.

در این مقاله با بررسی احراز هویت کاربران بانکی، روش مناسبی با استفاده از بیومتریک اثرانگشت، و رمز نگاری آن با روش رمزنگاری جریان پیشنهاد می‌شود.

۲. کاربرد بیومتریک در احراز هویت

امضاء یکی از ابتدایی‌ترین روش‌های احراز هویت است. در این روش امضای کاربر با امضای ثبت شده در سیستم بانکی مطابقت داده می‌شود، ولی این روش به‌صورت گسترده قابل استفاده نیست و عواملی چون خطای انسانی و جعل، امنیت این روش را زیر سوال می‌برند.

کلمه بیومتریک از کلمه یونانی بیو[3] به معنای زندگی و کلمه متریک[4] به معنای اندازه‌گیری تشکیل شده است. بیومتریک به روش‌های خودکار تشخیص یا تایید هویت[5] یک شخص زنده از طریق اندازه‌گیری مشخصه‌های فیزیولوژیکی یا رفتاری وی اطلاق می‌شود. بدین ترتیب بیومتریک یک مجموعه فناوری محسوب می‌گردد. [۱]

در علم بیومتریک اعضایی از بدن مورد توجه است که استفاده از آنها راحت‌تر و کم ضررتر باشد. ویژگی‌های فردی، چیزهایی است که هیچگاه گم، دزدیده و یا فراموش نمی‌شوند. همیشه و همه جا با فرد همراه هستند و به همین دلیل کارشناسان این شیوه‌ی شناسایی را بسیار ایمن‌تر و مطمئن‌تر از هر روش دیگری می‌دانند. واژه بیومتریک به طیف وسیعی از فناوری‌هایی اتلاق می‌شود که هویت افراد را به کمک اندازه‌گیری و تحلیل خصوصیات انسانی شناسایی می‌کنند. هر خصوصیت فیزیولوژیکی یا ویژگی رفتاری منحصر به فرد و متمایز کننده، مقاوم و قابل سنجش که بتواند جهت تعیین یا تأیید خودکار هویت افراد بکار رود بیومتریک نام دارد.

با وجود منحصر به فرد بودن خصوصیات بیومتریک برای جلوگیری از کلاهبرداری و... نیاز به فن‌آوری مناسب جهت ضبط احراز هویت را دارد. [2,3,4]

۲-۱ بخش‌های منطقی یک سیستم بیومتریک

یک سیستم بیومتریک از لحاظ منطقی به دو بخش تقسیم می‌شود:

۱- **نام نویسی**[6]: جمع‌آوری خصیصه‌ی بیومتریکی فرد و ذخیره آن در سیستم است. در این فاز ویژگی مورد نظر خوانده شده و پس از استخراج، در قالب الگوهایی جدا در بانک داده قرار می‌گیرد.

1 Online Banking
2 On Time Biometrics
3 Bios
4 Metrikos
5 Verification
6 Enrollment

۲- **شناسایی**[7]: وظیفه این بخش، تشخیص و تایید هویت افراد در هنگام ورود یا دستیابی به سیستم است. در این فاز بخش بیومتریک خوان، خصیصه بیومتریکی را خوانده و ویژگی آن را استخراج کرده و با الگوهای موجود در بانک داده مقایسه و درنهایت مجوز ورود یا عدم ورود به سیستم را صادر می‌کند.

۲-۲ گروه‌بندی روش‌های بیومتریک

روش‌های بیومتریک به سه گروه اصلی تقسیم شده‌اند:

۱- **شیمیایی**[8] : شامل ***DNA***[9] ، قندخون، بوی بدن، الگوی‌خونی

۲- **رفتاری**[10] : شامل راه رفتن، فشردن دکمه، صدا و امضاء

۳- **فیزیکی**[11] : شامل اثر انگشت، الگوی عنبیه چشم، الگوی حرارتی صورت و یا الگوی فیزیکی چهره، الگوی عروق خونی شبکیه چشم، هندسه دست، الگوی خطوط کف دست، گوش، بینی، حرکت لب، حرکت چشم، ناخن و...

۲-۳ سیستم‌های بیومتریک

تمامی سیستم‌های بیومتریک دارای یک معماری کلی یکسان، در ساخت هستند:

درخواست داده‌ها، پردازش سیگنال، تطبیق، تصمیم گیری، فضای ذخیره سازی، محیط انتقال داده‌ها، زیرسیستم که در آن داده‌های خامی که از یک فرد توسط یک سنسور ویژه اسکن شده است، وارد سیستم می‌شود. ترتیب فرایندی که در زیر سیستم انجام می‌شود عبارتست از:

- **دریافت داده‌ها توسط سنسور**
- **تبدیل‌داده‌های دریافتی از سنسورها به فرم مناسب برای ارسال به زیر سیستم پردازش‌سیگنال**

عملیات زیر سیستم پردازش سیگنال، به شرح ذیل می‌باشد:

۱- دریافت داده‌های خام از زیر سیستم جمع آوری داده

۲- استخراج خصیصه

۳- عملیات فیلترینگ جهت حذف نویز

۴- اصلاح داده‌ها

۵- تبدیل داده‌های دریافتی به فرم لازم (تولید الگو) برای زیر سیستم تطبیق.

داده‌های دریافت شده در این زیر سیستم، پس از پردازش، یک الگو از برخی ویژگی‌های موجود تولید و ذخیره می‌شود. در واقع این الگوی تولید شده مورد مقایسه و شناسایی قرار می‌گیرد. ماهیت این الگو که از روی یک شابلون[12] از پیش تعریف شده تولید می‌شود (یک استاندارد[13] ثابت) که ماتریسی از صفر و یک است. در واقع شابلون قسمت‌های مورد اندازه گیری از یک نمونه را برمی‌گرداند.

زیرسیستم تطبیق: فرایندی که طی آن میزان شباهت دو اثر انگشت اندازه‌گیری می‌شود. در اکثر سیستم‌ها از دو شاخه‌ها برای تطبیق دادن دو اثر انگشت استفاده می‌شود. در روشی موسوم به بانک فیلتر[14] ابتدا تصویر اثر انگشت به بخش‌هایی تقسیم شده، سپس در هربخش فیلتری موسوم به فیلتر گابور[15] را با زوایای مختلف اعمال کرده و به ازای هر زاویه انحراف معیار برای ناحیه مورد نظر محاسبه می‌شود.[5]

سیستم‌های تطبیق مبتنی بر دو شاخه می‌توانند به یکی از این دو شیوه عمل کنند:

---

7 Identification
8 Chemical Biometrics
9 Deoxy Ribonucleic Acid
10 Behavioral Biometrics
11 Physical Biometrics
12 Stencil
13 Standard
14 Filter Bank
15 Gabor Filter

- **تطبیق نقاط:** موقعیت مکانی، نوع دوشاخه و جهت لبه‌ای که دوشاخه بر روی آن قرارگرفته به عنوان خصوصیات اثرانگشت ذخیره شده و سپس در فاز تطبیق بررسی می‌شود که چند دو شاخه به خصوصیات یکسان بر روی هم ردیف می‌شوند.
- **تطبیق ساختار:** در این روش، به موقعیت مکانی دو شاخه‌ها توجهی نمی‌شود بلکه ساختار اطراف آن یا به عبارت دیگر نوع دوشاخه‌ها، به عنوان خصوصیات که در همسایگی یک دوشاخه قراردارند، تطبیق می‌شوند.

خروجی این زیر سیستم تطبیق، از مقایسه دو الگو بدست می‌آید. فرایند این زیر سیستم شامل: دریافت داده‌های پردازش شده(الگو) قبلی و الگوهای ذخیره شده و مقایسه آنها با الگوهای موجود است.

زیر سیستم تصمیم‌گیری: بعد از فراخوانی وظیفه آن تصمیم گیری بر روی تطابق انجام شده متناسب با درخواست است. در این مرحله یک حد یا آستانه برای تایید کاربر در نظر گرفته شده است.

زیر سیستم فضای ذخیره‌سازی: شامل الگوهایی است که در هنگام ثبت نام از کاربران بدست آمده است. ممکن است برای هر کاربر یک یا چند الگو ذخیره شده باشد.

زیر سیستم محیط انتقال: وظیفه این بخش انتقال داده‌ها، بین اجزاء یک سیستم بیومتریک است.

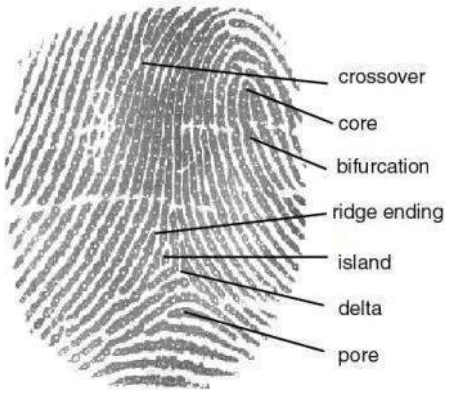
۳. اثر انگشت

اثر انگشت، متداول‌ترین روش در علم بیومتریک است. در سر انگشت هر فرد، الگویی از خط‌ها و شیارها وجود دارد که به آنها خطوط اصطکاکی[16] نیز می‌گویند. با این خطوط، حس لامسه[17] در تماس با اشیاء افزایش می‌یابد. این متد از قدیمی‌ترین آزمایش‌های تشخیص هویت است. زیرا این خطوط برای هریک از انگشتان دست هر فرد منحصر به فرد و غیر قابل تغییر است.

۳-۱ روش‌های تحلیل اثر انگشت

برای به حداقل رساندن داده‌های یک اثر انگشت در بانک اطلاعاتی، همه‌ی تصویر به طور کامل نگهداری نمی‌شود. نخست کل تصویر تحلیل شده و سپس نقاط کلیدی آن ذخیره می‌شود. این کار نقش بسیار مهمی برای جستجوی سریع در بانک‌های اطلاعاتی دارد. در مجموع هر تصویر اثرانگشت حدود ۳۵ ویژگی مهم مانند نقاط تقاطع، نقاط پایانی، انشعاب و... دارد.

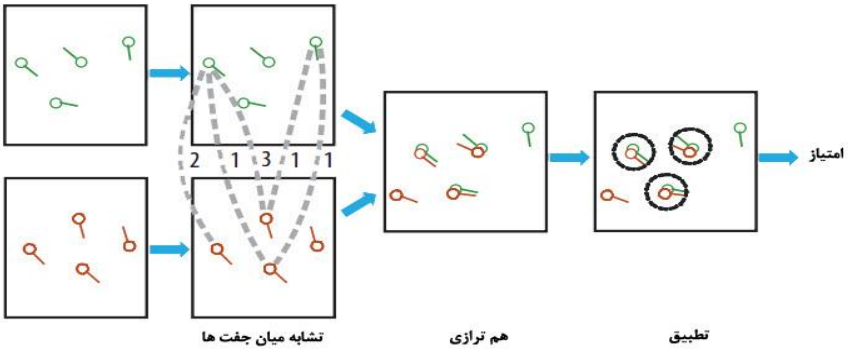
برای تشخیص هر اثر انگشت و اعلام آن با قطعیت بررسی ۸ تا ۲۲ ویژگی کافی است. مشخصات اثر انگشت یا به طور مستقیم روی ایستگاه یا روی کارت‌های هوشمند یا روی یک سرویس دهنده ذخیره می‌شود و در صورت تطابق مشخصات دریافتی با مشخصات ذخیره شده نسبت به صدور مجوز تصمیم‌گیری می‌شود.



شکل1 : محل نقاط ویژه در اثر انگشت

این روش در علم بیومتریک ***MBFM***[18] نامیده می‌شود. در این شیوه پردازش سنگینی روی تصویر برای استخراج مشخصات کلیدی انجام می‌گیرد. روش دیگری بنام ***CBFM*** [19] نیز وجود دارد که در آن به جای مقایسه تک تک نقاط کلیدی با داده‌های اصلی، بخش‌هایی از تصویر با بخش‌های متناظر از شکل اصلی مقایسه می‌شود.

16 Friction Ridge
17 Sense of touch, tactile sensation
18 Minutiae-Based Fingerprint Matching (MBFM)

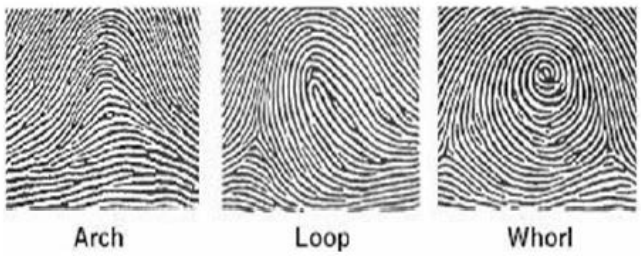


شکل۲ : الگوریتم تطبیق دو اثر انگشت[6]

۳-۲ تقسیم بندی ویژگی‌های اثر انگشت

الگوی اثر انگشت، انواع مختلفی از ویژگی‌ها را دارد که در سه کلاس کلی طبقه‌بندی شده‌اند:

- ✓ مارپیچی
- ✓ حلقه‌ای
- ✓ کمانی



شکل۳ : نمونه‌ای از طبقه‌بندی الگوهای اثر انگشت[7]

۳-۲-۱ تطبیق اثر انگشت

در مورد تطبیق، روش‌های گوناگونی وجود دارد که از جمله می‌توان به موارد ذیل اشاره کرد:

- تطبیق مجموعه نقاط
- تطبیق گراف
- همشکلی دو زیرگراف

البته عمل تطبیق بنا به دلایل زیر نیاز به محاسبات پیچیده دارد:

- معمولاً کیفیت اثر انگشت پایین است.
- بانک اطلاعاتی اثر انگشت‌ها بزرگ است.
- تصویرهایی که به صورت ساختاری آسیب دیده اند، به الگوریتم‌های نیرومندی جهت تطبیق نیاز دارند.

19 Correlation Based Fingerprint Matching (CBFM)

شکل۴ : اثر انگشت و قالب ذخیره‌سازی

۴. احراز هویت پیام‌ها و رمزنگاری

به جهت اهمیت و حساسی بودن داده‌های بیومتریک و مقابله با سرقت و جعل آنها، نیاز است تا به صورت رمز شده ذخیره و جابجا شوند. رمزنگاری علم شناخت و بررسی روش‌های ذخیره و بازیابی اطلاعات به صورت امن می‌باشد. که با استفاده از علوم ریاضیات، امنیت را برقرار می‌کند.

احراز هویت پیام نیز از روش‌های زیر انجام می‌گیرد:

✓ رمزنگاری متقارن[۲۰] : داده‌ها در مبداء با کلید متقارن مشترک بین مبداء و مقصد رمز می‌شوند. مقصد با رمزگشایی[۲۱] پیام با همان کلید از مبداء پیام مطمئن می‌شود. زیرا کس دیگری کلید را نمی‌داند. [8,9]

✓ رمزنگاری کلید عمومی[۲۲] : داده‌ها در مبداء با کلید خصوصی[۲۳] رمز می‌شوند. مقصد با رمزگشایی پیام با کلید عمومی از مبداء پیام مطمئن می‌شود.

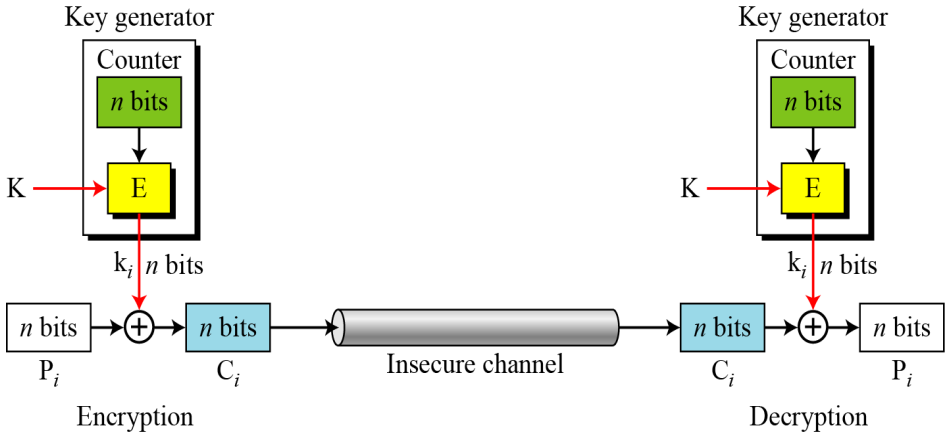
✓ استفاده از کد احراز هویت(اصالت) پیام[۲۴] ***MAC*** : یک کد اصالت سنجی پیام یا کد احراز هویت پیام عبارت است از تکه‌ی کوچکی از اطلاعات که برای اصالت سنجی یک پیام استفاده می‌شود.

✓ استفاده از توابع درهم‌سازی[۲۵] : همانند ***MAC*** بوده و تابع درهم‌سازی است که یک پیام با طول متغیر را به عنوان ورودی دریافت کرده و یک خروجی با طول ثابت و مشخص به عنوان کد درهم‌سازی را تولید می‌کند، برخلاف ***MAC***، از کلید استفاده نمی‌کند.

۵. رمزنگاری جریان[۲۶]

تکنیک رمزگذاری جریان بطور منحصر بفردی ارقام باینری یک پیام را در یک زمان با استفاده از یک انتقال رمز، در زمان‌های متفاوت، رمز می‌کند. رمزگذاری جریان غالباً در سخت‌افزار سریعتر از رمزگذاری قطعه‌ای (بلوکی) بوده و مدارهای ساده‌ای نیز دارد.

20 Symmetric Cipher(Symmetric Algorithm)
21 Decryption
22 Public Key Cipher
23 Private Key
24 Message Authentication Code (MAC)
25 Hash Function
26 Stream Cipher



شکل۵ : حالت ***CTR***[۲۷] به عنوان رمزنگاری جریان

با مولد اعداد تصادفی، یک رمز جریان می‌تواند به اندازه‌ی یک رمز قالبی با همان طول کلید، امن باشد. مزیت اصلی رمز جریان این است که تقریباً همیشه سریع‌تر و نسبت به رمز قالبی از حجم برنامه کمتری تشکیل می‌شود.

۶. سابقه‌ی کارهای انجام شده

جهت ارائه خدمات بانکی امن هویت بیومتریک[۲۸] ***MOC*** کاربرد فراوانی دارد. داده‌های بیومتریکی موجود در کارت شناسائی هوشمند ملی[۲۹] قابل استفاده بوده و امکان صدور گواهی هویت بیومتریک، امضای دیجیتال و... را جهت تصدیق هویت افراد میسر کرده است.

برای رفع نواقص موجود در سیستم‌های پرداخت بانکی به صورت برخط تدابیر زیادی توسط محققان اندیشیده شده است. ترکیبی از رمزنگاری و بیومتریک روش مناسبی برای حل مشکلات موجود و جلوگیری از حملات در سیستم‌های وابسته به اینترنت است.

۶-۱ سیستم اعتبارسنجی بیومتریک پرداخت الکترونیکی

سیستم برای بهبود امنیت خرید با کارت اعتباری در خصوص پروتکل‌های تجاری جهت معاملات الکترونیکی طراحی شده است. و از بیومتریک برای افزایش امنیت برخط معاملات مبتنی بر گوشی تلفن همراه جهت بالا بردن اعتماد مشتری در امنیت معاملات از راه دور، به عنوان واسط دیجیتالی استفاده شده است. [10]

این سیستم در ابتدا اطلاعات را به بارکد[۳۰] تبدیل کرده و با دستکاری پیکسلی آنها و تغییرات به بارکد و آرایه‌های بایت تبدیل می‌کند. در پایان، با استفاده از الگوریتم ***RSA***[۳۱]، رمزگذاری انجام می‌پذیرد.[11]

این مکانیزم فقط برای تراکنش موبایلی طراحی شده و در جایی که مشتری گوشی تلفن در دست ندارد، کاربردی ندارد. این سیستم ممکن است در صورت سرقت گوشی موبایل با خطر کپی برداری اثرانگشت و لو رفتن اطلاعات حساب مشتری همراه باشد.

۶-۲ امنیت آنلاین تراکنش‌های الکترونیکی

در این تحقیق محققان به بررسی معاملات الکترونیکی امن[۳۲] ***SET*** پرداخته و آن را به عنوان پروتکلی مهم در تجارت الکترونیکی معرفی نموده و مکانیسم بیومتریک را برای افزایش امنیت معامله برخط با دستگاه تلفن همراه مدل کرده‌اند.[12]

27 Click Through Rate (CTR)
28 Match On Card (MOC)
29 e_ID Card
30 Bar Code
31 Rivest Shamir Adleman (RSA)
32 Secure Electronic Transaction (SET)

۷. روش پیشنهادی

هریک از کارهای پیشین با روشی مناسب سعی بر امن کردن سیستم تبادلات بانکی به وسیله‌ی روش‌های مختلف و ترکیب آن با یک بیومتریک پرداختند. هریک با وجود مزایا، معایبی نیز دارند. در این قسمت سعی می‌شود برخی از نواقص موجود برطرف و سیستم امن‌تری را با احراز هویت اثر انگشت و رمزنگاری جریان بررسی و پیشنهاد شود.

۷-۱ مراحل روش پیشنهادی احراز هویت بیومتریک

پروتکل احراز هویت پیشنهادی از داده‌های بیومتریک استفاده می‌کند که باید از طریق ثبت با یک دستگاه (اثرانگشت خوان) خوانده و بایک الگوریتم محافظ، از الگو محافظت شود. پروتکل پیشنهادی با استفاده از ویژگی اثر انگشت، بسیار دقیق بوده و می‌تواند برای هر روش دیگر بیومتریکی استفاده شود. در حقیقت این روش ترکیبی از روش احراز هویت مبتنی بر کلمه عبور و روش بیومتریک اثر انگشت می‌باشد. و در واقع می‌توان گفت یک روش دو عامله است. این روش شامل مراحل زیر است:

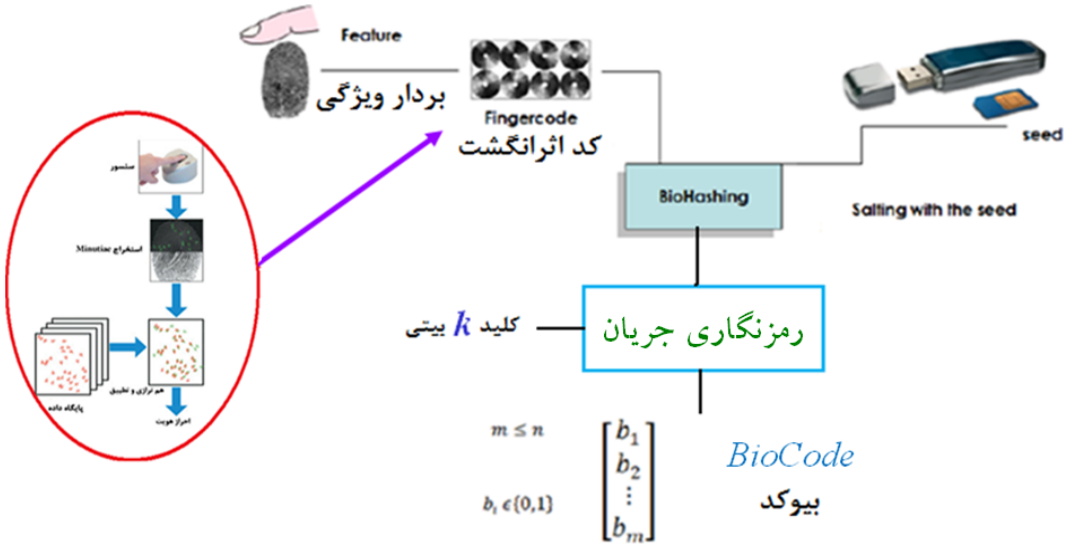
۷-۱-۱ پروتکل پیشنهادی استخراج بیوکد[۳۳]

این پروتکل شامل مراحل زیر است:

الف) استخراج کد اثر انگشت

در یکی از شعب بانک با دریافت اثر انگشت مشتری با حسگر دستگاه ثبت اثرانگشت و طی مراحل پردازش تصویر، یک بردار ویژگی بنام کد اثر انگشت استخراج خواهد شود. برای ذخیره‌ی داده‌های اثرانگشت دریافتی از مشتری در پایگاه‌داده با تجزیه و تحلیل بیومتریک آن از یک الگوریتم درهم‌ساز[۳۴] استفاده خواهد شود.

شکل زیر مراحل استخراج بیوکد را به تصویر کشیده است:



شکل۷: مراحل پیشنهادی استخراج بیوکد

ب) استخراج تابع به وسیله الگوریتم درهم‌سازی

کد اثرانگشت همراه با کلمه عبور از جعبه‌ی رمزنگاری و تابع درهم ساز گذر می‌کند که خروجی آن یک بیوکد است.

توابع درهم ساز از لحاظ امنیتی قابلیت‌هایی را دارند:

- ✓ برگشت ناپذیر و یکطرفه[۳۵]: یعنی برای یک h ورودی، یافتن x به گونه‌ای که $H=h(x)$ ازلحاظ محاسباتی ناممکن[۳۶] است.
- ✓ مقاوم در برابر تصادم ضعیف[۳۷] : برای یک x داده شده(معلوم)، بایستی یافتن y به گونه‌ای که $H(y)=H(x)$ از لحاظ محاسباتی ناممکن باشد.

33 BioCode
34 Biohashing
35 One - Way
36 Infeasible

- ✓ مقاوم در برابر تصادم قوی[۳۸] : یافتن x و y (هردو نامعلوم) به گونه‌ای که $H(y)=H(x)$ از لحاظ محاسباتی ناممکن باشد.
- ✓ طول ورودی آن متفاوت.
- ✓ طول خروجی آن ثابت (نگاشت از فضای بزرگ به کوچک)
- ✓ مقاوم در برابر تصادم (احتمال یافتن پیام‌های متفاوتی که با یک رشته یکسان نگاشته شوند دشوار است.)
- ✓ رشته‌ی فوق، چکیده یا عصاره پیام[۳۹] است.
- ✓ در حالت کلی، کلیدی وجود ندارد.

ج) درهم‌سازی

این تابع، تابعی از استانداردهای رمزنگاری جریان است. جعبه رمزنگاری هم می‌تواند با کلیدی اشتراکی، بین پذیرنده و بانک به صورت مشترک باشد. از طرفی رمز عبور نیز که ممکن است مستقیماً در اختیار مشتری باشد و یا در یک قفل تعبیه و ذخیره شود. بیوکد نیز در مراحل ثبت و یا احراز هویت کاربر استفاده می‌شد.

۷-۱-۲ پروتکل پیشنهادی فاز ثبت نام

برای دریافت اثر انگشت، مشتری با داشتن مدرک هویتی برای یک بار در یکی از شعب بانک حضور می‌یابد. کارمند بانک با دریافت اثر انگشت به ذخیره و جمع‌آوری قالب مرجع که می‌تواند به هر اسمی نامیده شود، می‌پردازد. در این پروتکل قالب اولیه توسط یک بیوکد بنام مرجع[۴۰] بیوکد از یک کدانگشت با بردار ویژگی خاص و یک رمز که با شماره سریال دستگاه ثبت اثرانگشت، همراه است، شناخته می‌شود. کلمه عبور نیز یک رمز یا یک مقدار تصادفی ذخیره شده در دستگاه است، که به وسیله‌ی تایید بیومتریک دستگاه محافظت می‌شود. پس از محاسبه‌ی مرجع بیوکد، از طریق یک کانال ***SSL***[۴۱] به پایگاه داده بانک ارسال و در آنجا ذخیره می‌شود. تا در مراحل خرید و احراز هویت مورد استفاده قرار گیرد.

۷-۱-۳ پروتکل پیشنهادی فاز احراز هویت

وقتی در یک فروشگاه توسط خریدار تقاضای پرداخت برخط ارسال می‌شود، بانک باید اثر انگشت فرد متقاضی را با قالب مرجع، مقایسه و تایید نماید. لذا برای این عمل چالشی به پایگاه داده مرجع ارسال کرده و با قالب مرجع شامل اثرانگشت و رمز عبور مشتری است، مقایسه و پاسخ رد یا قبول ارائه نماید. که برای این کار بیوکد ثبت شده، کدانگشت موجود در داده‌های بیومتریک، رمز عبور و شماره سریال دستگاه ثبت اثرانگشت، محاسبه می‌کند.

تقاضای ثبت بیوکد با استفاده از الگوریتم درهم‌سازی در کپچر[۴۲] بیوکد با چالش ارسالی توسط بانک به عنوان رمز محاسبه می شود.[13]

بانک نیز با کمک تابع درهم‌ساز، بیوکد دریافتی را با به چالش کشیدن الگوریتم با بیوکد مرجع محاسبه می‌کند.

۸. تجزیه و تحلیل و ارزیابی مطالب

در این قسمت کارایی عملکرد و خطاهای سیستم ثبت اثر انگشت و پروتکل پیشنهادی محاسبه خواهد شد:

۸-۱ کارایی عملکرد

با توجه به اینکه برای ارزیابی عملکرد دستگاه‌های بیومتریک معیار یکتایی وجود ندارد. لذا جهت بیان قابلیت‌های سیستم‌های بیومتریک، بایستی چندین معیار محاسبه و بررسی شوند.

۸-۱-۱ خطاهای موجود در سیستم‌های ثبت اثر انگشت

37 Weak Collision
38 Strong Collision
39 Digest
40 Reference
41 Secure Socket Layer (SSL)
42 Capture

برای محاسبه‌ی کارایی این سیستم‌ها براساس نرخ تشخیص مثبت اشتباه ***FPIR***[۴۳] و نرخ تشخیص منفی اشتباه ***FNIR***[۴۴] که می‌توان به طور مجزا آنها را اندازه‌گیری نمود. می‌توان گفت تشخیص مثبت اشتباه، زمانی رخ می‌دهد که سیستم برای بررسی یک اثر انگشت ثبت نشده، نتیجه مثبتی را ارائه دهد.

تشخیص منفی اشتباه نیز وقتی است که سیستم برای اثر انگشت ثبت شده، نتیجه منفی یعنی تطبیق اشتباه و یا عدم تطبیق را برگرداند. ارتباط بین این دو مقوله از رابطه زیر حاسب می‌شود:

$$FPIR = 1 - (1 - FMR)^N$$ رابطه(۱)

N ، تعداد کاربران ثبت شده در یک سیستم است. و هر چه تعداد آنها افزایش یابد، میزان نرخ تطابق اشتباه ***FMR***[۴۵] شدیداً کاهش می‌یابد تا کارایی سیستم درحد مطلوب حفظ شود.

۸-۱-۲ تجزیه و تحلیل عملکرد اثر انگشت

عملکرد روش پیشنهادی را در این قسمت برای جلوگیری از رد اشتباه نادرست بررسی می‌شود.

در اینجا از سه پایگاه داده اثر انگشت به صورت استاندارد استفاده شده است. عملکردهای بهترین الگوریتم‌ها با نرخ خطای برابر[۴۶] ***EER*** و نرخ پذیرش اشتباه ***FMR*** روی این سه پایگاه داده در جدول۱ محاسبه شده است. در این جدول ***ZeroFRM*** زمانی که هیچ مورد اشتباهی پذیرفته نشده باشد به عنوان مقدار نرخ عدم تطابق اشتباه[۴۷] ***FNMR*** خواهد بود.

جدول۱: عملکرد بهترین الگوریتم برای سه پایگاه داده

DataBase	*EER*	*Zero FMR*
CASIA V3	*٪۱۴0.*	*٪۲۰0.*
CASIA V4	*٪۳۰0.*	*٪۶۶0.*
CASIA V5	*٪۱۳1.*	*٪۴۲2.*

در این محاسبات دیده می‌شود که نرخ خطای برابر ***EER*** بسیار کم و درحد صفر درصد است.

۹. نتیجه گیری

این روش برای استفاده و امنیت در هر نوع سیستم پرداخت آنلاین قابل بهره برداری است، که شامل استفاده از مکانیسم اعتبارسنجی بیومتریک بوده و برای تایید هویت از قالب ذخیره شده‌ی اثر انگشت در زمان ثبت نام استفاده می‌شود. که در صورت انطباق اثر انگشت با نمونه‌ی اولیه در پایگاه داده، پرداخت الکترونیکی وجه موفق آمیز خواهد شد و مشتری قادر به انجام معامله و خرید خواهد شد و به راحتی امنیت در سیستم‌های برخط برقرار می‌شود.

پروتکل پیشنهادی به آسانی جهت حفظ امنیت و حصول اطمینان کافی در پرداخت‌های الکترونکی تاثیر دارد. سیستم پیشنهادی ارائه شده دارای امنیت، قابلیت اتصال به ***ATM***[۴۸] و هر دستگاه دیگری را دارد. از طرف دیگر الگوریتم رمزنگاری جریان، با دارا بودن مزیت‌های مختلف زیر:

قابلیت پیاده‌سازی سریع، پیاده‌سازی ساده‌ی نرم‌افزاری، حجم پایین، پیچیدگی کم و امنیت بالا برای ابزارهایی با منابع محدود بسیار کاربردی خواهد بود.

43 False Positive Identification Rate (FPIR)
44 False Negative Identification Rate (FNIR)
45 False Match Rate (FMR)
46 Equal Error Rate (EER)
47 False Non Match Rate (FNMR)
48 Automated Teller Machine (ATM)

۱۰.پیشنهادهای آتی

با توجه به اینکه اکثر مشتریان بانکی، برای کارت‌های خود اغلب از رمز عبور راحت، مثل سال تولد، شماره شناسنامه یا اعداد رند و ساده استفاده می‌کنند که به راحتی می‌تواند حدس و گمانه‌زنی شده و یا هک شوند، نیاز به احراز هویت‌های مختلف بیومتریک احساس می‌شود. از طرفی درحال حاضر افراد در هرجا و همه وقت از تلفن‌های همراه استفاده می‌کنند، لذا بیومترک همراه و آنلاین در پرداخت از طریق تلفن همراه یکی از گزینه‌های ساده برای معامله برخط پیشنهاد می‌شود. روش‌های جدید و مناسب‌تر، استفاده از بیومتریک‌های چندگانه بجای رمز عبور مثل گفتار، ریتم وارد کردن رمز، عنبیه، هندسه دست و... می‌توانند پیشنهادهای خوبی باشند.

منابع

[1] Ratha, N. K., Connell, J.H, and Bolle, R.M .2010. Enhancing Security and Privacy in Biometric Based Authentication System. IBM Systems Journal, 40(3), pp. 615-634.
[2] Biometrika, 2011. Introduction to Biometric Systems, s.l.: Biometrika (Italy) Available at:http://www.biometrika.it/ eng/wp_biointro.html.
[3] French, T. 2012. CIS050-6 Week 6: Biometrics. , Luton Campus, UK: University of Bedfordshire. Available at: http://breo.beds.ac.uk.
[4] Stanley, P., Jeberson, W., and Klinsega V.V. 2009. Biometric Authentication: A Trustworthy Technology for Improved Authentication. 2009 International Conference on Future Networks, , pp. 171-175.
[5] Mahajan, S. and Singh, M. (2014) Analysis of RSA Algorithm Using GPU Programming. arXiv:1407.1465 [cs.CR]
[6] Agrawal, M. and Mishra, P. (2012) A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering, 4, 877.
[7] Anil K. Jain, Patrick Flynn, Arun A. Ross, Handbook of Biometric (Springer Science+ Business Media, LLC, 2008).
[8] William Stalling, 'Cryptography and Network Security: Principles and Practice, 6th Edition, Pearson,2014.
[9] Behrouz A. Forouzan,' Cryptography and Network Security', 2017 McGraw-Hill Global Education Holdings, LLC. All rights reserved.
[10] MarketPlace, A. 2011. Nigerian bank deploys country's first biometric ATM, s.l.: ATM MarketPlace,Available on: http://www.atmmarketplace.com/article/179366/Nigerian-bank-deploys-country-s-first-biometric-ATM.
[11] Nikhil Khandare, Dr.B.B.Meshram. International Journal of Reserch and Applications e-HSSN:2320-8163, Volume1, Issue 5 (Nov-Dec 2013),pp,53-58.
[12] Nikhil Khandare, Dr. B. B. Meshram, International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 1, Issue 5 (Nov-Dec 2013), PP. 53-58
[13] Pornin, T. (2013) Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA).