INSO
16371
1st. Edition
Jun.2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۶۳۷۱
چاپ اول
خرداد ۱۳۹۲

فناوری اطلاعات- فنون امنیتی –

محافظت از اطلاعات زیست‌سنجی

Information technology— Security techniques — biometric information protection

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند.

در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
«فناوری اطلاعات – فنون امنیتی – محافظت از اطلاعات زیست‌سنجی»

رئیس:	**سمت و/یا نمایندگی**
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا : (اسامی به ترتیب حروف الفبا)	
ابریشمی، سعید (دکترای کامپیوتر)	عضو هیات علمی دانشگاه فردوسی مشهد
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس سازمان فناوری اطلاعات ایران
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	مشاور سازمان فناوری اطلاعات ایران

فیاضی، مهدی (لیسانس مهندسی الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قندهاری، آزاده (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس مؤسسه تحقیقات ارتباطات و فناوری اطلاعات
قهرمانی، معصومه (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس مرکز آمار و کامپیوتر دانشگاه فردوسی مشهد
قهرمانی، مرضیه (لیسانس مهندسی کامپیوتر نرم افزار)	نماینده دانشگاه فردوسی مشهد
معروف، سینا (لیسانس مهندسی کامپیوتر سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران
موجبی، محمود (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استاندارد ها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات – فنون امنیتی – محافظت از اطلاعات زیست‌سنجی» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در دویست و سومین اجلاس کمیته‌ی ملی استاندارد رایانه و فراوری داده ها مورخ ۱۳۹۱/۸/۱۴ مورد تصویب قرارگرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

این استاندارد ملی برمبنای استاندارد بین‌المللی زیر تدوین شده و معادل آن به زبان فارسی است:

ISO/IEC 27475:2011, Information technology— Security techniques —Biometric information protection

مقدمه

همان‌گونه که اینترنت به‌بخشی از زندگی روزانه نفوذمی‌کند، خدمات مختلفی از جمله بانکداری اینترنتی، مراقبت‌های بهداشتی از دور، و غیره نیز از طریق آن ارائه می‌گردد. برای ارائه این خدمات به یک روش امن، نیاز به سازوکارهای احراز هویت بین افراد و خدمات در حال ارائه، حیاتی‌تر می‌شود. برخی از سازوکارهای احراز هویت در حال حاضر عبارتند از شِماهای مبتنی بر نشانه[1]، شماره‌های شناسایی و تراکنش شخصی (PIN[2] / TAN[3])، شِماهای امضای دیجیتال مبتنی بر سامانه‌های رمزنگاری کلید عمومی و شِماهای احراز هویت با استفاده از فنون زیست‌سنجی.

زیست‌سنجی‌ها – بازشناسی خودکار افراد بر اساس مشخصه‌های رفتاری و فیزیولوژیکی شان- اکنون به مرحله بلوغ رسیده‌اند و شامل فن‌آوری‌های بازشناسی مبتنی بر تصویر اثر انگشت، الگوهای صدا، تصویر عنبیه، تصویر چهره و مانند آن می‌باشد. هزینه فنون زیست‌سنجی در حال کاهش است، در حالی که قابلیت اطمینان آن‌ها افزایش یافته است، و در حال حاضر هردوی این عوامل برای استفاده به عنوان سازوکار احراز هویت، قابل قبول و ماندگار می‌باشند.احراز هویت

1-Token
2 -Personal identification number
3 Transaction Number

مبتنی بر زیست‌سنجی یک ناسازگاری بالقوه بین حفظ حریم خصوصی[1] و تضمین احراز هویت را نشان می‌دهد. از یک طرف، هامشخصه‌های زیست‌سنجی به‌طور ایده‌آل، یک ویژگی غیرقابل تغییر منتسب و متمایز برای هر فرد هستند. این مقیدکردن اعتبارنامه به شخص، تضمین قوی از احراز هویت را فراهم می‌کند. از سوی دیگر، این انقیاد قوی همچنین زمینه‌ساز نگرانی‌های حریم خصوصی مرتبط با استفاده از زیست‌سنجی هم می‌باشد، مانند پردازش غیر قانونی داده‌های زیست‌سنجی، و باعث ایجاد چالش‌هایی در زمینه امنیت سامانه‌های زیست‌سنجی برای جلوگیری از به‌خطر افتادن مراجع زیست‌سنجی می‌گردد. در احراز هویت زیست‌سنجی، به‌طورکلی راه‌حل معمول برای مساله به خطر افتادن یک اعتبارنامه احراز هویت - تغییر رمز عبور و یا صدور نشانه جدید - وجود ندارد، چراکه تغییر مشخصه‌های زیست‌سنجی، چه از نوع خواص ذاتی فیزیولوژیکی، و چه عادات رفتاری افراد باشند، دشوار یا غیر ممکن است. حداکثر می‌توان از یک انگشت و یا یک چشم دیگر استفاده کرد، اما انتخاب‌ها معمولا محدود هستند. بنابراین، اقدامات متقابل مناسب برای حراست از امنیت یک سامانه زیست‌سنجی و حفظ حریم خصوصی موضوعات داده‌ها ضروری است.

سامانه‌های زیست‌سنجی معمولا یک مرجع زیست‌سنجی را به سایر اطلاعات قابل شناسایی شخصی (PII)[2] به‌منظور تصدیق هویت افراد مقید می‌کنند. در این صورت، انقیاد باید امنیت رکورد[3] حاوی اطلاعات زیست‌سنجی را تضمین کند. افزایش پیوند مراجع زیست‌سنجی با دیگر PII و به اشتراک گذاری اطلاعات زیست‌سنجی در بین حوزه‌های قضایی قانونی، تضمین حفاظت از اطلاعات زیست‌سنجی و انطباق با مقررات مختلف حفظ حریم خصوصی را برای سازمان‌ها بسیار دشوار ساخته است.

1 -Privacy
2- Personally Identifiable Information
3 -Record

فناوری اطلاعات- فنون امنیت – محافظت از اطلاعات زیست‌ستجی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، ارائه راهنماهایی برای حفاظت از اطلاعات زیست‌سنجی تحت الزامات مختلف برای محرمانگی، یکپارچگی، و تجدیدپذیری یا ابطال‌پذیری، در حین ذخیره سازی و انتقال است. علاوه بر این، این استاندارد ملی الزامات و راهنماهایی برای مدیریت و پردازش امن و سازگار با حفظ حریم خصوصی اطلاعات زیست‌سنجی ارائه می‌کند.

این استاندارد ملی موارد زیر را مشخص می‌کند:

- تحلیل تهدیدات و اقدامات متقابل ذاتی در یک زیست‌سنجی و مدل‌های کاربرد سامانه زیست‌سنجی؛
- الزامات امنیتی برای انقیاد امن یک مرجع زیست‌سنجی و یک هویت مرجع۱؛
- مدل‌های کاربرد سامانه‌های زیست‌سنجی با سناریوهای مختلف برای ذخیره‌سازی و مقایسه مراجع زیست‌سنجی؛ و
- راهنمایی در حفاظت از حریم خصوصی یک فرد در هنگام پردازش اطلاعات زیست‌سنجی.

این استاندارد ملی، مسائل مدیریت عمومی مربوط به امنیت فیزیکی ، امنیت زیست محیطی و مدیریت کلید برای فنون رمزنگاری را شامل نمی‌شود،

مراجع الزامی [۲]

۲ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می رود:

۲-۱
احراز هویت[۳]

فرآیند ایجاد یک سطح مورد توافق از اطمینان نسبت به اصالت یک هستار خاص و یا یک هویت مورد ادعا

یادآوری ۱– احراز هویت شامل فرآیند تعیین یک سطح مورد توافق از اطمینان از درستی یک هویت مورد ادعا، قبل از ثبت و به رسمیت شناخته شدن هستار در یک دامنه می‌باشد.

---

1 -Identity Reference

۲ -این استاندارد دارای مراجع الزامی نیست.

3 -Authentication

یادآوری ۲- اگر چه این تعریف عمومی است، استفاده از آن در این استاندارد ملی، محدود به احراز هویت زیست‌سنجی موضوعات انسانی می‌باشد.

[ISO 19092:2008]

۲-۲ داده‌های کمکی[1]

AD

داده‌های وابسته به موضوع که بخشی از یک مرجع تجدید پذیر زیست‌سنجی می‌باشند و ممکن است در هنگام درستی سنجی، و یا به‌طورکلی برای درستی سنجی در بازسازی شناساگرهای مستعار ، مورد نیاز باشند.

یادآوری ۱- اگر داده‌های کمکی بخشی از یک مرجع تجدید پذیر زیست‌سنجی باشند، به‌طور الزامی در همان مکان شناساگرهای مستعار مربوطه ذخیره نمی‌شوند .

یادآوری۲- داده‌های کمکی ممکن است برای تنوع، شامل عناصر داده (یعنی داده‌های متنوع) باشند.

یادآوری۳- داده‌های کمکی در هنگام درستی سنجی مرجع زیست‌سنجی، عنصر مورد مقایسه نیستند.

یادآوری۴- داده‌های کمکی به‌وسیله سامانه‌های زیست‌سنجی در هنگام ثبت نام، تولید می‌شوند

مثال: عدد محرمانه رمزشده به‌وسیله یک کلید که از یک نمونه زیست‌سنجی با استفاده از یک روش داده‌های کمکی به‌دست آمده است، شِمای تعهد فازی ، یا جهش فازی. برای دیدن مثالهای واقعی از PI و AD، به جدول ت۱ از پیوست ت مراجعه کنید.

۲-۳ مشخصه زیست‌سنجی[2]

مشخصه‌های فیزیولوژیکی یا رفتاری یک فرد که می‌توانند تشخیص داده شده و از آن‌ها، ویژگی‌های زیست‌سنجی متمایزکننده، تکرارپذیر به‌منظور بازشناسی خودکار افراد، استخراج گردد.

---

1 - Auxiliary data

2 - BioMetric characteristic

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

۲-۴ داده‌های زیست‌سنجی[۱]

نمونه زیست‌سنجی ، ویژگی زیست‌سنجی، مدل زیست‌سنجی، خصیصه زیست‌سنجی، داده‌های توصیفی دیگر برای مشخصه‌های زیست‌سنجی اصلی یا اجتماع داده‌های بالا.
[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

۲-۵ موضوع داده زیست‌سنجی[۲]

موضوع
فردی که مرجع زیست‌سنجی وی درون سامانه زیست‌سنجی قرار دارد.

۲-۶ ویژگی زیست‌سنجی[۳]

اعداد یا برچسب‌هایی که از نمونه‌های زیست‌سنجی استخراج شده و برای مقایسه استفاده می‌گردند.
[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

۲-۷ حفظ حریم خصوصی اطلاعات زیست‌سنجی[۴]

حق کنترل جمع‌آوری، انتقال، استفاده، ذخیره‌سازی، بایگانی، از بین بردن و تجدید اطلاعات زیست‌سنجی شخصی یک فرد در طی چرخه زندگی وی.

۲-۸ مدل زیست‌سنجی[۵]

تابع ذخیره شده (وابسته به موضوع داده زیست‌سنجی) که از روی یک ویژگی یا ویژگی‌های زیست‌سنجی تولید شده است.

Biometric Data
2 - Biometric data subject

3 - Biometric feature

4 - Biometric information privacy

5 - Biometric model

یادآوری- عمل مقایسه، تابع ذخیره شده را به ویژگی‌های زیست‌سنجی یک نمونه زیست‌سنجی مورد آزمایش اعمال می‌کند تا یک امتیاز مقایسه به‌دست بدهد.

مثال نمونه‌هایی از توابع ذخیره شده عبارتند از مدل‌های پنهان مارکوف[1]، مدل‌های مخلوط گاوسی[2] یا شبکه‌های عصبی مصنوعی

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

۲-۹ خصیصه زیست‌سنجی[3]

ویژگی‌های توصیفی موضوع داده زیست‌سنجی که به‌وسیله ابزارهای خودکار، از روی نمونه زیست‌سنجی تخمین زده شده و یا بدست آمده‌اند.

مثال اثر انگشت‌ها می‌توانند با ویژگی‌های زیست‌سنجی جریان-لبه (یعنی قوس، پیچ و انواع حلقه‌ها) طبقه‌بندی شوند. تصاویر چهره‌ها می‌توانند برای تخمین سن و جنسیت استفاده شوند.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

۲-۱۰ مرجع زیست‌سنجی BR[4]

یک یا چند نمونه زیست‌سنجی، الگوی زیست‌سنجی، و یا مدل زیست‌سنجی ذخیره‌شده که به یک موضوع داده زیست‌سنجی منسوب شده و برای مقایسه استفاده می‌گردند.

یادآوری- یک مرجع زیست‌سنجی که می‌تواند تجدید شود، به عنوان یک مرجع تجدیدپذیر زیست‌سنجی نامیده می‌شود.

مثال تصویر چهره در گذرنامه، الگوی جزئیات اثر انگشت بر روی یک کارت شناسایی ملی، مدل مخلوط گاوسی برای بازشناسی گوینده در یک پایگاه داده .

[ISO/IEC JTC ۱/SC ۳۷ SD۲ (v.۱۱)]

1 -Hidden Markov Model
2 -Gaussian Mixture Models
3 - Biometric property
4 - Biometric reference

۲-۱۱ نمونه زیست‌سنجی[1]

نمایش قیاسی و یا رقمی مشخصه‌های زیست‌سنجی که از یک دستگاه اخذ زیست‌سنجی[2] یا یک زیرسامانه اخذ[3] زیست‌سنجی، قبل از استخراج ویژگی‌های زیست‌سنجی به‌دست آمده است.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

۲-۱۲ سامانه زیست‌سنجی[4]

سامانه‌ای با هدف بازشناسی خودکار افراد براساس مشخصه‌های فیزیولوژیکی و رفتاری آن‌ها.

۲-۱۳ الگوی زیست‌سنجی[5]

مجموعه‌ای از ویژگی‌های زیست‌سنجی ذخیره شده که قابلیت مقایسه مستقیم با ویژگی‌های زیست‌سنجی مورد آزمایش را دارا می‌باشند.

۲-۱۴ ادعا[6]

اعلان کردن هویت

۲-۱۵ مدعی[7]

فرد اعلان کننده یک هویت

یادآوری- ادعاها به روش‌های متعددی قابل درستی‌سنجی هستند که ممکن است برخی از آن‌ها برمبنای زیست‌سنجی باشند.

۲-۱۶ شناساگر مشترک[8]

شناساگر ای برای مرتبط کردن هویت‌های مرجع و مراجع زیست‌سنجی در پایگاه‌داده‌هایی که از لحاظ فیزیکی یا منطقی از یکدیگر جدا هستند.

---

1 - Biometric sample
2 Biometric capture device
3 -Capture
4- Biometric system
5- Biometric template
6 - Claim
7 - Climant
8 - Common identifeir

۲-۱۷ متنوع سازی[1]

ایجاد عمدی چندین مرجع زیست‌سنجی تبدیل یافته، و مستقل از روی یک یا چند نمونه زیست‌سنجی به‌دست آمده از یک موضوع داده منفرد، به‌منظور بهبود امنیت و حفظ حریم خصوصی.

۲-۱۸ شناسایی[2]

<زیست‌سنجی> فرآیند یک جستجوی زیست‌سنجی در یک پایگاه داده ثبت‌نام، برای پیدا کردن و بازگرداندن هویت مرجع منتسب به یک فرد واحد.

۲-۱۹ شناساگر[3]

یک یا چند صفت که به‌طور یکتا یک هستار را در یک دامنه خاص، مشخص می‌نماید.

مثال‌ها نام یک باشگاه به همراه یک شماره عضویت باشگاه، شماره کارت بیمه درمانی به همراه نام شرکت بیمه‌گر، یک آدرس IP و یک شناساگریکتای جهانی.

۲-۲۰ هویت[4]

مجموعه ای از خصیصه‌ها یا مشخصه‌های یک هستار که می‌تواند برای توصیف وضعیت، ظاهر و یا سایر مشخصات آن به‌کار رود.

۲-۲۱ سامانه مدیریت هویت[5]

IdMS

سامانه‌ای که اطلاعات هویتی هستار را در طی چرخه حیات آن اطلاعات در یک دامنه کنترل می‌نماید.

---

1 - Diversification
2 - Identification
3 - Identifier
4 - Identity
5 - Identity management system
-

۲-۲۲ هویت مرجع[1]

IR

یک صفت غیر زیست‌سنجی یعنی شناساگری حاوی یک مقدار که در طی دوره وجود هستار در یک دامنه،ثابت می‌ماند.

۲-۲۳ بازگشت‌ناپذیری[2]

ویژگیی از یک تبدیل که از روی نمونه (ها) یا ویژگی‌های زیست‌سنجی، یک مرجع زیست‌سنجی می‌سازد، به‌طوری‌که دانستن مرجع زیست‌سنجی تبدیل‌شده[3] ، نمی‌تواند برای تعیین هر اطلاعاتی درباره تولید نمونه (ها) و یا ویژگی‌های زیست‌سنجی،به‌کار رود.

۲-۲۴ اطلاعات قابل‌شناسایی شخصی[4]

PII

هرگونه اطلاعاتی که

- شخصی را که اطلاعات متعلق به وی است، شناسایی می‌کند، و یا می‌تواند برای شناسایی، برقراری تماس، و یا پیداکردن آن شخص مورد استفاده قرار گیرد.
- از آن‌ها اطلاعات شناسایی و یا تماس یک فرد مشخص می‌تواند به‌دست آید، یا
- به طور مستقیم یا غیر مستقیم به یک فرد عادی مرتبط است یا می‌تواند مرتبط گردد. [ISO/IEC 29100: 1)]

۲-۲۵ شناساگر مستعار[5]

PI

قسمتی از یک مرجع زیست‌سنجی تجدیدپذیرکه یک شخص یا موضوع داده را در یک دامنه مشخص، با استفاده از یک هویت محافظت‌شده که می‌تواند از طریق یک نمونه زیست‌سنجی اخذشده و داده‌های کمکی(در صورت وجود) درستی‌سنجی شود، نشان می‌دهد.

---

1 - Identity reference
2 - Irreversibility
3-Transformed biometric reference
4 - Personally identifiable information

5 Pseudonymous identifier

یادآوری ۱ - یک شناساگر مستعار، فاقد هرگونه اطلاعاتی است که اجازه بازیابی نمونه زیست‌سنجی اصلی، ویژگی‌های زیست‌سنجی اصلی، یا هویت اصلی صاحبش را بدهد.

یادآوری ۲ - شناساگر مستعار در خارج از دامنه خدمت، بی‌معنا است.

یادآوری ۳- داده‌های زیست‌سنجی رمزنگاری شده با یک رمز۱ که اجازه بازیابی داده‌های متن اصلی[۲] را می‌دهند، یک شناساگر مستعار نیستند.

یادآوری۴- یک شناساگرمستعار، عنصر مورد مقایسه در حین درستی‌سنجی مرجع زیست‌سنجی، می‌باشد.

یادآوری ۵- برای دیدن مثالهایی از PI و AD به جدول ت۱ در پیوست ت، مراجعه کنید.

۲-۲۶ کدبندی‌کننده شناساگر مستعار[۳]

PIE

سامانه، فرآیند یا الگوریتمی که یک مرجع تجدید پذیر زیست‌سنجی متشکل از یک شناساگر مستعار (PI) و در صورت امکان داده‌های کمکی (AD) را براساس یک نمونه زیست‌سنجی یا الگوی زیست‌سنجی تولید می‌کند.

۲-۲۷ تجدیدپذیری[۴]

خاصیتی از یک تبدیل و یا یک فرآیند برای ایجاد چندین مرجع زیست‌سنجی تبدیل شده مستقل، که از یک یا چند نمونه زیست‌سنجی به دست‌آمده از یک موضوع داده یکسان، مشتق شده و می‌توانند برای بازشناسی آن فرد، بدون افشای اطلاعات مربوط به مرجع اصلی، به‌کار روند.

۲-۲۸ مرجع زیست‌سنجی تجدید پذیر[۵]

شناساگر ابطال‌پذیر یا تجدیدپذیر که یک فرد یا موضوع داده را در یک دامنه مشخص، با استفاده از یک هویت دودویی محافظت شده که از روی یک نمونه زیست‌سنجی اخذشده، ساخته شده (بازسازی شده) است، بازنمود می‌کند.

یادآوری- یک مرجع تجدیدپذیر زیست‌سنجی از یک شناساگرمستعار و عناصر داده ای اختیاری اضافی، که همانند داده‌های کمکی، مورد نیاز برای درستی‌سنجی یا شناسایی مبتنی بر زیست‌سنجی هستند، تشکیل می‌شود.

---

1 -Cipher
2 Plain text
3 - Pseudonymous identifier encoder
4 - Renewability
5 - Renewable biometric reference

۲-۲۹ ابطال‌پذیری[1]

قابلیت جلوگیری از درستی‌سنجی موفقیت‌آمیز یک مرجع خاص زیست‌سنجی و هویت مرجع مربوط به آن، در آینده می‌باشد.

یادآوری- رد یک هستار ممکن است بر اساس حضور آن در یک لیست ابطال رخ دهد.

۲-۳۰ کانال امن[2]

کانال ارتباطی که محرمانگی و اعتبار پیام‌های مبادله‌شده را تامین می‌کند.

۲-۳۱ نشانه[3]

دستگاه فیزیکی که مرجع زیست‌سنجی را ذخیره کرده و در برخی موارد مقایسه زیست‌سنجی را به‌صورت برروی صفحه[4] انجام می‌دهد.

مثال‌ها کارت هوشمند، حافظه[5] گذرگاه سری جهانی[6] **(USB)**یا شناسه فرکانس رادیویی(RFID)[7] در گذرنامه الکترونیکی

۲-۳۲ پیوندناپذیری[8]

ویژگی دو یا چند مرجع زیست‌سنجی که نمی‌توانند با یکدیگر، یا با موضوعی(موضوعاتی)که از آن به‌دست آمده‌اند، پیوند داشته باشند.

---

1 - Revocability
2 - Secure channel
3 - Token
4 -On-board
5 -Memory Stick
6 -Universal Serial Bus
7 -Radio Frequency Identification
8 - Unlinkability

۲-۳۳ درستی‌سنجی[1]

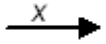
<زیست‌سنجی> فرآیند تایید یک ادعا مبنی براینکه فردی که موضوع یک فرآیند اخذ زیست‌سنجی است، منبع یک مرجع هویت مورد ادعا می‌باشد.

۳ کوته نوشت‌ها

AD	Auxiliary Data	داده‌های کمکی
AFIS	Automated Fingerprint Identification Systems	سامانه‌های شناسایی خودکار اثرانگشت
BR	Biometric Reference	مرجع زیست‌سنجی
BIR	Biometric Information Record	رکورد اطلاعاتی زیست‌سنجی
CI	Common Identifier	شناساگر مشترک
OCC	Card Comparison-On	مقایسه درکارت
DBBR	Database containing Biometric Reference	پایگاه داده حاوی مرجع زیست‌سنجی
DBIR	Database containing Identity Reference	پایگاه داده حاوی هویت مرجع
IdMS	Identity Management System	سامانه مدیریت هویت
IR	Identity Reference	هویت مرجع
MAC	Message Authentication Code	کد تایید اصالت پیام
PDA	tPersonal Digital Assistan	دستیار رقمی شخصی
PET	Privacy Enhancing Technology	فناوری بهبود حفظ حریم خصوصی
PI	Pseudonymous Identifier	شناساگر مستعار
PIC	Pseudonymous Identifier Comparator	مقایسه‌گر شناساگر مستعار
PIE	Pseudonymous Identifier Encoder	کدبندی‌کننده شناساگر مستعار
PII	Personally Identifiable Information	اطلاعات قابل‌شناسایی شخصی
PIR	Pseudonymous Identifier Recoder	ثبت‌کننده شناساگر مستعار
RBR	Renewable Biometric Reference	مرجع زیست‌سنجی تجدیدپذیر

1 - Verification

RFID	Radio Frequency Identification	شناسایی فرکانس رادیویی
TTP	rusted Third PartyT	طرف سوم مورداعتماد
USB	Serial Bus Universal	گذرگاه سری جهانی
UUID	Universal Unique Identifier	شناساگر یکتای جهانی


یک پیکان که یا نمایش‌دهنده یک جریان اطلاعات ساده از داده x ، و یا نمایش‌دهنده آغاز یک پروتکل[1] تعاملی است که داده‌های مبادله شده آن ممکن است به همه و یا بخشی از x وابسته باشد.

یادآوری ۱– هنگامیکه از یک سامانه پیغام رسانی امن مانند ISO/IEC 7816-4 استفاده می‌شود، مجاز است x رمزگذاری شود

یادآوری ۲– هنگامی‌که، به‌عنوان مثال، از یک فن دانش-صفر[2] استفاده می‌گردد، پروتکل تعاملی مجاز نیست هیچ اطلاعاتی را بر روی **x** منتقل نماید.

۴ سامانه‌های زیست‌سنجی

۴-۱ معرفی سامانه‌های زیست‌سنجی

سامانه‌های زیست‌سنجی، بازشناسی خودکار افراد را بر اساس یک یا چند مشخصه فیزیولوژیکی (صفات فیزیکی بدن مانند اثر انگشت) و/یا رفتاری (کارهایی که یک نفر انجام می‌دهد مانند راه رفتن) انجام می‌دهند. مشخصه‌های فیزیولوژیکی شامل موارد زیر می‌باشد، گرچه تنها محدود به این موارد نیست:

- اثر انگشت،
- چهره،
- عنبیه،
- هندسه دست،
- رگ دست / انگشت،
- شبکیه،
- DNA، و
- اثر کف دست

1 -Protocol
2 Zero Knowledge

و مشخصه‌های رفتاری شامل موارد زیر می‌باشد، گرچه تنها محدود به این موارد نیست:

- امضا،
- روش راه رفتن، و
- صدا

موارد زیر ویژگیهای مطلوبی از مشخصه‌های زیست‌سنجی هستند که منجر به تمایز خوب موضوع (فرد) و انجام بازشناسی قابل اطمینان می‌شوند [۴]:

- جهانی بودن : هر فرد باید آن مشخصه را داشته باشند؛
- یکتایی: هر فرد باید یک مشخصه قابل تمایز داشته باشد؛
- پایداری: مشخصه‌ها نباید تغییری را در زمان نشان دهند ، به‌عنوان مثال در طول زمان تغییر نکنند؛
- قابلیت جمع آوری: مشخصه‌ها باید بتوانند به سادگی از موضوعات جمع آوری شوند؛ و
- تکرارپذیری: برای بازشناسی موفقیت‌آمیز موضوع، مشخصه‌ها باید به اندازه کافی متمایز و تکرارپذیر باشند.

از نقطه‌نظر کاربردی، خواص افزونه زیر نیز باید به حساب آورده شود:

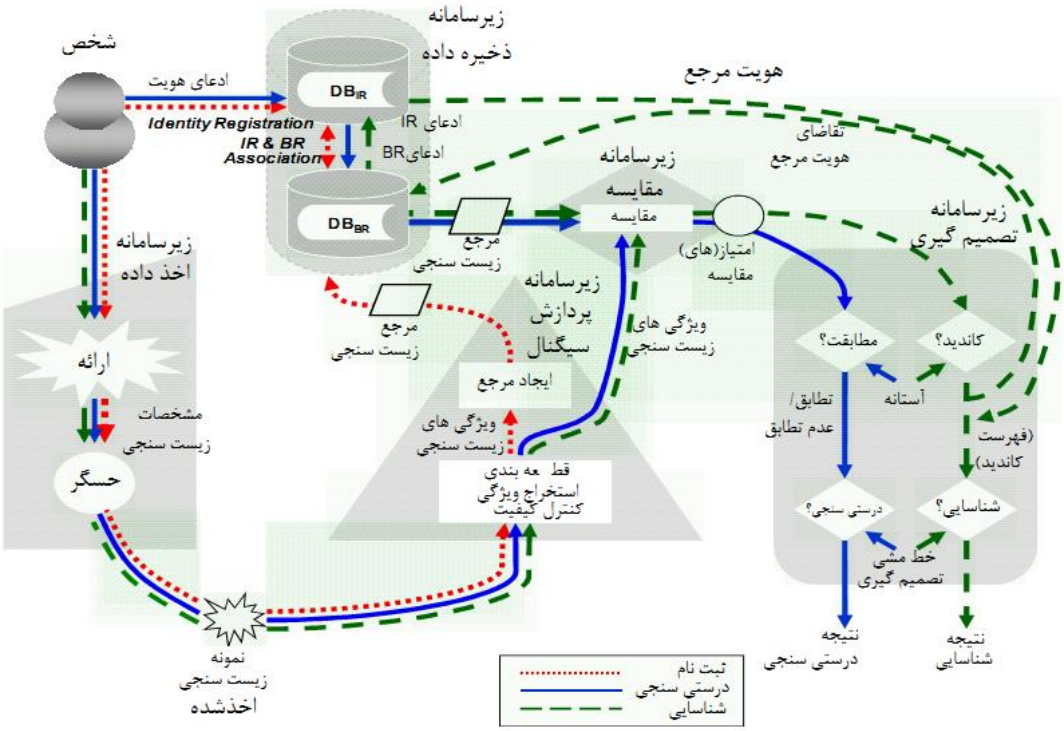
- کارآیی، که عمدتا به میزان موفقیت در شناسایی افراد اشاره دارد؛
- قابلیت پذیرش، که نشان‌دهنده سطح تمایل موضوع به استفاده از سامانه زیست‌سنجی دارد و
- مقاومت در برابر کلاه برداری، که نشان‌دهنده میزان دشواری استفاده از یک همتا از مشخصه زیست‌سنجی برای فریب دادن سامانه زیست‌سنجی است.

برای درستی‌سنجی و/یا شناسایی یک شخص، یک سامانه زیست‌سنجی یک یا چند نمونه گرفته شده[1] را برای مقایسه با مرجع(های) زیست‌سنجی ذخیره شده، پردازش می‌کند. مرجع زیست‌سنجی می‌تواند یک نمونه زیست‌سنجی (به‌عنوان مثال یک تصویر که نشان دهنده مشخصه زیست‌سنجی است) و یا مجموعه ای از ویژگی‌های زیست‌سنجی (یعنی، یک الگو که از روی تصویر به‌دست آمده است) و یا یک مدل زیست‌سنجی که از ترکیب ویژگیها تشکیل شده است، باشد. مخصوصا، تغییر مشخصه‌های زیست‌سنجی فیزیولوژیکی بسیار دشوار است، بنابراین به خطر افتادن آن‌ها

1 -Probe samples

می‌تواند عواقب ابدی برای فرد موردنظر، در کاربردهایی که مشخصه در آن‌ها غیرقابل تغییر فرض شده است، در بر داشته باشد.

۲-۴ عملیات سامانه زیست‌سنجی



شکل ۱ – ساختار مفهومی یک سامانه زیست‌سنجی

عمل کلی یک سامانه زیست‌سنجی در شکل ۱ نشان داده شده است، که نسخه توسعه یافته‌ای از نسخه اصلی ارائه شده در استاندارد ISO/IEC SC37 SD11، [۱۸] برای برجسته کردن پردازش هویت مرجع می‌باشد.

معمولا سامانه زیست‌سنجی شامل پنج زیر سامانه می‌باشد:

- یک زیرسامانه اخذ داده زیست‌سنجی، که حاوی تجهیزات اخذ زیست‌سنجی یا حسگرهایی برای جمع‌آوری سیگنال‌ها از یک مشخصه زیست‌سنجی و تبدیل آن‌ها به یک نمونه زیست‌سنجی مانند یک تصویر اثر انگشت، تصویر چهره یا صدای ضبط‌شده می‌باشد.

- یک زیرسامانه پردازش سیگنال، که ویژگی‌های زیست‌سنجی را از یک نمونه زیست‌سنجی استخراج می‌کند، به این منظور که اعداد یا برچسب‌هایی را محاسبه نماید که بتوانند با موارد استخراج‌شده از سایر نمونه‌های زیست‌سنجی مورد مقایسه قرار گیرند. در اینجا ویژگی زیست‌سنجی استخراج شده در فرآیند ثبت نام، به‌عنوان یک مرجع زیست‌سنجی برای فرآیند شناسایی و درستی سنجی، در زیرسامانه ذخیره‌سازی داده‌ها، ذخیره می‌شود.

- یک زیر سامانه ذخیره‌سازی داده‌ها، که در درجه اول به‌عنوان یک پایگاه داده ثبت نام که پیوند مراجع زیست‌سنجی ثبت نام شده با هویت مرجع در آن برقرار می‌گردد به‌کار می‌رود. داده‌ها مجاز هستند شامل اطلاعات زیست‌سنجی و همچنین داده‌های غیر-زیست‌سنجی مانند هویت مرجع مربوط به موضوع باشند. به دلیل نگرانیهای امنیتی و حفظ حریم خصوصی، اغلب DBIR و DBBR در عمل به‌صورت منطقی یا فیزیکی از هم جدا می‌شوند. توصیف جزئی‌تر نحوه انقیاد DBIR با DBBR در ضمیمه الف آورده شده است.

- یک زیرسامانه مقایسه، که میزان شباهت بین نمونه‌های زیست‌سنجی اخذشده (یا ویژگیهای مشتق‌شده از آن‌ها) و مراجع زیست‌سنجی ذخیره شده را تعیین می‌نماید. در مورد مقایسه یک به یک که در فرآیند درستی‌سنجی به‌کار می‌رود، یک نمونه زیست‌سنجی اخذشده با یک مرجع زیست‌سنجی ذخیره‌شده از یک موضوع داده زیست‌سنجی مقایسه می‌گردد تا یک امتیاز مقایسه ایجاد گردد. اما در مقایسه یک به چند که در فرآیند شناسایی به‌کار می‌رود، یک ویژگی استخراج شده از یک موضوع داده زیست‌سنجی، با مجموعه ای از مراجع زیست‌سنجی متعلق به بیش از یک موضوع داده زیست‌سنجی مقایسه می‌گردد تا مجموعه‌ای از امتیازات مقایسه، برگردانده شود.

- یک زیرسامانه تصمیم، که تعیین می‌کند آیا نمونه زیست‌سنجی اخذشده و مرجع زیست‌سنجی، بر اساس یک امتیاز(های) مقایسه و یک خط مشی (یاخط مشی‌های) تصمیم‌گیری دارای یک آستانه، دارای منبع (موضوع زیست‌سنجی) یکسان هستند. در مورد فرآیند درستی‌سنجی، موضوع داده زیست‌سنجی مجاز است با توجه به امتیاز مقایسه، پذیرفته یا مردود شود. در مورد شناسایی، فهرستی از هویت‌های نامزد که منطبق بر خط‌مشی تصمیم گیری هستند، ارائه می‌گردند.

در اصل، یک سامانه زیست‌سنجی شامل سه فرآیند کارکردی اصلی است:

- فرآیند ثبت نام: ایجاد و نگهداری یک سند داده ثبت نام برای فردی که موضوع یک فرآیند اخذ زیست‌سنجی، مطابق با خط‌مشی ثبت نام می‌باشد. معمولا موضوع، مشخصه‌های زیست‌سنجی خود را به همراه هویت مرجعش به یک حسگر ارائه می‌کند. نمونه زیست‌سنجی اخذشده پردازش می‌گردد و ویژگی‌های استخراج‌شده به‌عنوان یک مرجع، به‌همراه هویت مرجع در پایگاه داده ثبت نام، ثبت می‌گردند.

- فرآیند شناسایی: عبارت است از جستجو به دنبال ویژگیهای زیست‌سنجی اخذ و استخراج شده، برای برگرداندن یک فهرست از نامزدها. فهرست نامزدها متشکل از افرادی است که در زیرسامانه مقایسه، مراجع آن‌ها با

ویژگی موردنظر مطابقت داشته است، و مقدار امتیاز شباهت آن‌ها از یک مقدارآستانه از پیش تعریف شده، بیشتر می‌باشد.

- فرآیند درستی‌سنجی: آزمایش یک ادعا مبنی بر اینکه فردی که موضوع یک فرآیند اخذ زیست‌سنجی است، منبع یک مرجع زیست‌سنجی مشخص است. موضوع (فرد)، هویت مرجع و همچنین مشخصه‌های زیست‌سنجی(های) خود را برای یک ادعای هویت به دستگاه اخذ کننده ارائه می‌کند، که این دستگاه نمونه(های) زیست‌سنجی را به‌دست می‌آورد که برای مقایسه با مرجع زیست‌سنجی مربوطه به هویت مرجع مربوط به هویت ادعاشده، استفاده می‌شود.

در فرآیند درستی‌سنجی، امکان تحت تأثیر قرار گرفتن حریم خصوصی اطلاعات موضوع وجود دارد، چراکه این فرآیند نیاز به هر دو مرجع زیست‌سنجی و هویت مرجع دارد. فرآیند شناسایی نیاز به جستجوی کامل پایگاه داده ثبت نام دارد. بنابراین، این مسئله نیز امکان تأثیر بر حریم خصوصی فیزیکی موضوع را دارد. به‌طور کلی درستی‌سنجی نسبت به شناسایی، کمتر برای حریم خصوصی مزاحمت ایجاد می‌کند.

پنج زیرسامانه اشاره شده در بالا، نشان‌دهنده بلوک‌های فنی و کارکردی هستند که اعمال اخذ، پردازش، ذخیره، مقایسه، و تصمیم‌گیری را برروی داده‌های زیست‌سنجی انجام می‌دهند. علاوه‌براین، زیر سامانه‌های کارکردی دیگری نیز می‌توانند اضافه شوند [۷].

- یک زیرسامانه تطبیق-مرجع[1]، که یک مرجع را با استفاده از یک ویژگی جدید زیست‌سنجی که از یک فرآیند موفق درستی‌سنجی یا شناسایی استخراج شده است، تغییر می‌دهد. به‌طور کلی تطبیق به‌وسیله سامانه‌های زیست‌سنجی برای انعکاس عوامل خارجی و کمینه کردن تأثیرات آن‌ها بر روی نرخ بازشناسی به‌کار گرفته می‌شود. همچنین این زیرسامانه مجاز است برای تضعیف تاثیرات بالقوه سالخوردگی مرجع نیز استفاده شود. تطبیق نظارت‌نشده می‌تواند براساس یک خط‌مشی از پیش معین، به‌طور خودکار انجام شود. به‌طورکلی تطبیق نظارت‌شده به‌وسیله برنامه کاربردی درخواست می‌شود و مبتنی بر معیارهای مختص به برنامه کاربردی است. به‌عنوان مثال، تطبیق نظارت‌شده زمانی می‌تواند فراخوانی گردد که امتیاز مقایسه زیست‌سنجی زیاد نیست، اما عوامل دیگر هویت ادعاشده را به‌وضوح تایید می‌کنند. از آنجایی‌که یک امتیاز امتیاز مقایسه کمتر می‌تواند منجر به رد یک کاربر اصیل به‌وسیله سامانه شود، بهتر است استفاده از یک زیرسامانه تطبیق-مرجع در مراحل اولیه برپایی سامانه زیست‌سنجی در نظر گرفته شود.

1 -Reference-adaptaion subsystem

یک زیرسامانه مدیریتی، که کلیات خط‌مشی، پیاده‌سازی و بکارگیری سامانه زیست‌سنجی را برطبق محدودیت‌های قانونی، قضایی، و اجتماعی مرتبط، و همچنین الزامات حریم خصوصی، کنترل می‌کند. چند مثال توضیح‌دهنده عبارتند از:

-فراهم ساختن اطلاعات مرتبط با حفظ حریم خصوصی برای موضوع، در هنگام پردازش زیست‌سنجی؛

-ذخیره‌سازی و قالب‌دهی مراجع زیست‌سنجی و/یا داده‌های تبادل زیست‌سنجی؛

-تصمیم‌گیری بر روی سازوکارهای رمزگذاری و امضای دیجیتال برای محرمانگی و یکپارچگی اطلاعات قابل‌شناسایی شخصی (PII) حاوی داده‌های زیست‌سنجی؛

- تحلیل آسیب‌پذیریها، و حملات امنیتی علیه مجموعه سامانه زیست‌سنجی و پیاده‌سازی اقدامات متقابل مناسب؛

- فراهم ساختن داوری نهایی برروی خروجی تصمیم‌گیری‌ها و/یا امتیازات؛

- تنظیم مقادیر آستانه برای زیرسامانه تصمیم گیری؛

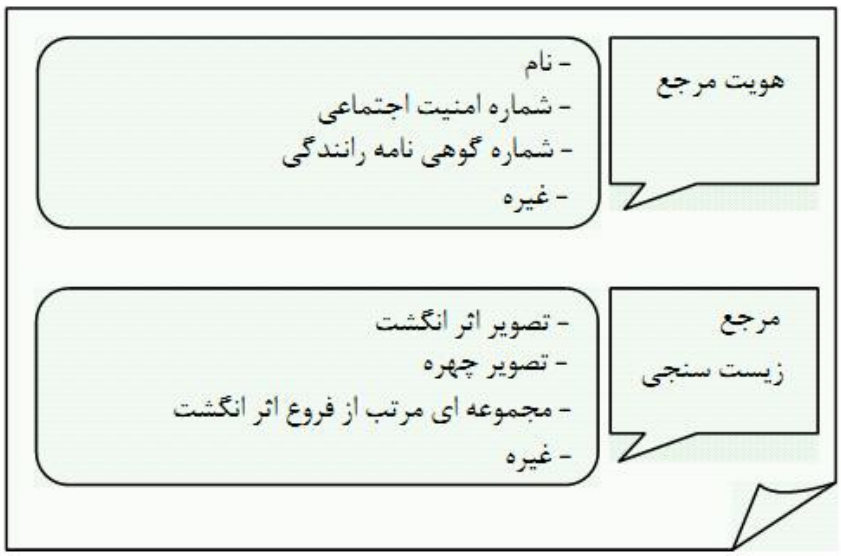
- کنترل محیط عملیاتی و ذخیره سازی داده‌های غیر زیست‌سنجی و

- فراهم ساختن حراست‌های مناسب برای حفظ حریم خصوصی موضوع.

۳-۴ مراجع زیست‌سنجی و مراجع هویت

یک فرد در هر دامنه مشخص، تنها یک شناساگر دارد اما ممکن است چندین مرجع هویت برای شناسایی آن فرد در آن دامنه وجود داشته باشد. هر مرجع هویت یک صفت، یا ترکیبی از صفات، از هویت یک هستار است که آن هستار را در یک دامنه خاص به صورت یکتا، شناسایی می‌کند. همچنین یک مرجع هویت می‌تواند ترکیبی از صفات فرد باشد.
یک مرجع زیست‌سنجی یکی از چندین صفات متعلق به یک فرد است که می‌تواند برای بازشناسی آن شخص درون یک دامنه مورد استفاده قرار گیرد. این استاندارد ملی، صفات هویتی را به دو دسته غیر زیست‌سنجی و زیست‌سنجی طبقه‌بندی می‌کند. برای سادگی، اولی به عنوان مرجع هویت (IR) و دومی به‌عنوان مرجع زیست‌سنجی (BR) نامیده می‌شوند. چندین نمونه از مراجع هویت و مراجع زیست‌سنجی در شکل ۲ نشان داده شده است، اگرچه این یک فهرست

جامع یا قطعی نیست. در اینجا، کادر محصورکننده نشان‌دهنده مجموعه ای از صفات است که مجازند برای شناسایی فرد مورد استفاده قرار گیرند.

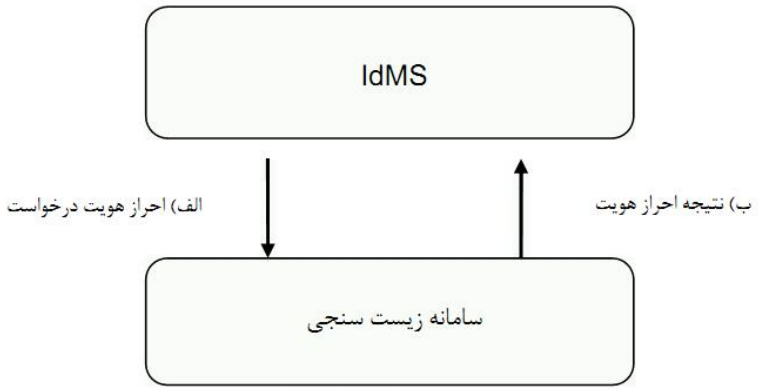


شکل ۲ - هویت‌های مرجع و مراجع زیست‌سنجی

۴-۴ سامانه‌های زیست‌سنجی و سامانه‌های مدیریت هویت

سامانه مدیریت هویت (IdMS)[1] وظیفه مهم اجتناب از تداخلات یا ابهامات هویتی را در هر دامنه به‌عهده دارد (برای جزئیات بیشتر درباره IdMS به IEC/SOI 24760-1 مراجعه کنید). یک سامانه احراز هویت نیازمند یک فرآیند شناسایی و درستی‌سنجی دقیق در یک دامنه (به خوبی تعریف شده)، و همچنین یک رابطه تعریف شده با فرآیندهای عضویت و ثبت نام می‌باشد که می‌توانند در همان دامنه باشند و یا از دامنه دیگری فراخوانی گردند. هنگامی‌که زیست‌سنجه‌ها برای فراهم‌ساختن یک خدمت احراز هویت بکار گرفته می‌شوند، IdMS مجاز است از سامانه زیست‌سنجی تقاضای احراز هویت کند (الف در شکل ۳) و سامانه زیست‌سنجی مجاز است نتیجه احراز هویت را به IdMS ارائه نماید (ب در شکل ۳).

1 -Identity management system



شکل ۳- سامانه زیست‌سنجی بعنوان یک ارائه دهنده سرویس احراز هویت برای IdMS

درخواست احراز هویت

۴-۵ اطلاعات قابل‌شناسایی شخصی و شناساگرهای یکتای جهانی

برخی از سامانه‌های زیست‌سنجی، نمونه‌های زیست‌سنجی مانند تصاویر چهره در گذرنامه‌های الکترونیکی را برای شناسایی مستقیم فرد استفاده می‌کنند، و برخی دیگر خصوصیات زیست‌سنجی مانند نقاط جزئی[۱] یک اثر انگشت و ضرایب چهره ویژه[۲] مربوط به یک چهره را برای شناسایی غیر مستقیم فرد منتسب به هویت مرجع استفاده می‌کنند. این قابلیت، یعنی توانایی پیوند داده‌های زیست‌سنجی به موضوع، مراجع زیست‌سنجی PII[۳] را ایجاد می‌کند. مراجع زیست‌سنجی این قابلیت را دارند که با توجه به متمایز بودنشان، به عنوان یک شناساگر یکتای جهانی (UUID)[۴] مورد استفاده قرار گیرند. یک UUID یک هویت مرجع است که می‌تواند برای پیوند اطلاعات شخصی در بین پایگاه‌های داده‌های مختلف مورد استفاده قرار گیرد، و در نتیجه باعث ایجاد یک تهدید بالقوه برای حفظ حریم خصوصی می‌گردد. به این ترتیب، نگرانی‌های قابل‌توجهی درباره استفاده از یک مرجع زیست‌سنجی به عنوان UUID مطرح شده است. به‌جز در مواردی که برای انجام این کار یک نیاز اثبات شده به طور واضح وجود دارد، بهتر است از مراجع زیست‌سنجی به عنوان یک شناساگر یکتای جهانی استفاده نشود.

UUID از آنجایی تبدیل به یک خطر بالقوه برای حفظ حریم خصوصی می‌شود که یک شخص می‌تواند در بین پایگاه‌داده‌های حاوی PII مربوطه تحت نظارت و ردیابی قرار گیرد. وقتی از مرجع زیست‌سنجی یا انقیاد آن با هویت مرجع استفاده می‌شود، می‌تواند به‌عنوان اطلاعات قابل شناسایی شخصی طبقه‌بندی گردد که ممکن است برای فرد، بسته به دامنه خاص، بسیار مهم باشد [۵]. اگر از پایگاه داده‌های UUID از داده‌های زیست‌سنجی استفاده می‌شود،

1 -minutiae
2 eignenface
3 -Personally identifiability information
4 -Universal unique identifier

بهتر است ملاحظاتی برای طراحی که الزامات ابطال‌پذیری و تجدیدپذیری را به‌منظور محدود کردن این مقایسه متقاطع[1] باشد، منظور گردد، به‌عنوان مثال، از طریق استفاده از مراجع متنوع‌شده همانگونه که در این استاندارد ملی تشریح شده است.

۶-۴ ملاحظات اجتماعی

همیشه استفاده از سامانه‌های زیست‌سنجی یک بعد اجتماعی دارد، جنبه‌هایی از آن ممکن است در الزامات قانونی مربوط به عملکرد این سامانه‌ها دیده شود (مانند مواردی‌که مربوط به حفاظت از اطلاعات شخصی می‌شوند)، درحالی‌که جنبه‌های دیگری همانند قابلیت پذیرش به‌وسیله موضوعات استفاده کننده از این سامانه‌ها بسیار دلخواه بوده و در کارآیی مناسب سامانه موثر است. قابلیت پذیرش یک سامانه ممکن است تحت تاثیر عوامل مذهبی، قومی، و فرهنگی، و همچنین عادات روانی فرد قرار داشته باشد.

در تمامی سامانه‌های زیست‌سنجی که مستقر شده‌اند، توصیه می‌شود افراد و سازمان‌های مسئول عملیات این سامانه‌ها توجه کنند که حفاظت از داده‌های زیست‌سنجی با سازوکارهای امنیتی مناسب، برای برآوردن الزامات قانونی (برای حفاظت از اطلاعات شخصی)، و همچنین کمک به پذیرش این سامانه‌ها به‌وسیله جامعه و افراد، ضروری است.

طراحان و متصدیان سامانه‌هایی که از زیست‌سنجی استفاده می‌کنند، بهتر است اطمینان حاصل کنند که تکالیف قانونی و تجربیات خوب مربوط به موارد زیر به‌خوبی درنظر گرفته شده است:

- سلامت و ایمنی؛
- دسترس پذیری، که تضمین می‌کند سامانه‌ها با یک تلاش فیزیکی و شناختی کم، برای طیف گسترده ای از جمعیت موجود به خصوص برای افراد ناتوان جسمی یا ذهنی قابل استفاده است، ؛ و
- قابلیت استفاده، که سامانه‌هایی موثر، کارآمد و رضایت بخش برای استفاده را ارائه می‌نماید.

بحث گسترده تر از ملاحظات اجتماعی و اداری و قضایی در برنامه‌های کاربردی تجاری، در ISO/IEC TR 24714-1 یافت می‌شود. [۱۹]

1 -Cross-comparison

۵ جنبه‌های امنیتی یک سامانه زیست‌سنجی

۵-۱ الزامات امنیتی برای سامانه‌های زیست‌سنجی به منظور حفاظت از اطلاعات زیست‌سنجی

۵-۱-۱ محرمانگی

محرمانگی، خصوصیتی است که اطلاعات را در مقابل دسترسی غیر مجاز یا فاش شدن، محافظت می‌نماید. در سامانه‌های زیست‌سنجی، یک مرجع زیست‌سنجی که طی فرآیند ثبت نام، در یک پایگاه داده مرجع زیست‌سنجی ذخیره شده است، در طی فرآیند درستی‌سنجی و شناسایی به زیرسامانه مقایسه منتقل می‌گردد . در طی این فرآیند، ممکن است هستارهای غیر مجاز به مرجع زیست‌سنجی دسترسی پیدا کنند، یعنی ممکن است مرجع زیست‌سنجی خوانده شده و یا اطلاعات هویتی مقید به آن فاش گردد. افشای غیر مجاز داده‌ها بدلیل حساسیت زیست‌سنجی‌ها می‌تواند منجر به تهدیدات حیاتی حفظ حریم خصوصی گردد. محرمانگی داده‌های ذخیره و منتقل شده زیست‌سنجی را می‌توان با سازوکارهای کنترل دسترسی و اشکال مختلف فنون رمزگذاری فراهم کرد.

یادآوری- اشکال مختلفی از الگوریتم‌های رمز نگاری، با استفاده از یک رمز متقارن و یا نامتقارن، می‌توانند برای تأمین محرمانگی داده‌ها بکار روند. برای اطلاعات بیشتر، پیوست ب.۱ را ببینید.

۵-۱-۲ یکپارچگی

یکپارچگی، خاصیت حراست از دقت و کامل بودن خصیصه‌ها است. یکپارچگی یک مرجع زیست‌سنجی، یک خاصیت حیاتی برای تضمین امنیت کل سامانه زیست‌سنجی است. یکپارچگی فرآیند احراز هویت بستگی به ی یکپارچگی مرجع زیست‌سنجی دارد. اگر مرجع زیست‌سنجی، و یا خصوصیات زیست‌سنجی اخذ و استخراج شده غیر قابل اعتماد باشند، احراز هویت حاصل نیز غیر قابل اعتماد خواهد بود. مراجع یا نمونه‌های غیرقابل اعتماد زیست‌سنجی به یک یا چند دلیل از موارد زیر می‌توانند رخ دهند:

- خرابی اتفاقی به‌دلیل عملکرد غلط سخت‌افزار یا نرم‌افزار

- تغییر اتفاقی یا عمدی یک مرجع زیست‌سنجی واجد شرایط به‌وسیله یک هستار مجاز (یعنی یک ثبت نام شده مجاز یا یک صاحب سامانه) بدون مداخله یک مهاجم.

- تغییر (از جمله جایگزینی)یک مرجع زیست‌سنجی مربوط به یک ثبت نام شده مجاز به‌وسیله یک مهاجم.

سامانه‌های زیست‌سنجی باید حفاظت موثر از یکپارچگی داده‌ها را به‌کار گیرند. این امر می‌تواند با بکارگیری سازوکارهای کنترل دسترسی که مانع از دسترسی غیر مجاز به داده‌های زیست‌سنجی می‌گردد، یا وارسی استفاده از

فنون رمزگذاری یکپارچگی محقق شود. ممکن است برای محافظت در مقابل استفاده مجدد از داده‌های زیست‌سنجی سرقت شده و حملات تکرار[1]، نیاز به ترکیب حفاظت از یکپارچگی با فنون دیگر (مانند مهرگذاری زمانی) باشد.

یادآوری ۱- فنون مختلف، از جمله کد احراز هویت پیام (MAC)[2] و یا امضای دیجیتالی را می‌توان برای تأمین یکپارچگی داده‌ها مورد استفاده قرار داد. برای اطلاعات بیشتر، به پیوست ب.۲ نگاه کنید

یادآوری ۲- برخی شرایط به هردوی محرمانگی و یکپارچگی نیاز دارند. اگر محافظت از محرمانگی و یکپارچگی هردو مورد نیاز هستند، یک راه ممکن استفاده از رمزگذاری و MAC یا امضای دیجیتال به طور همزمان است. امکان دیگر استفاده از رمزگذاری احراز هویت شده می‌باشد، مطابق آنچه در ISO/IEC 19772 [۱۶] استاندارد شده است.

یادآوری ۳- هنگامی که یک کارت هوشمند برای ذخیره و/یا مقایسه مرجع زیست‌سنجی مورد استفاده قرار می‌گیرد (بند ۸، مدلهای B، F ، G و H)، توصیه می‌شود از سازوکارهای امن پیام‌رسانی مطابق با استاندارد ISO/IEC 7816-4 [۳۰] برای یکپارچگی و/یا محرمانگی داده‌های زیست‌سنجی استفاده گردد.

۵-۱-۳ تجدیدپذیری و ابطال‌پذیری

یک نگرانی عمده امنیتی و حفظ حریم خصوصی برای سامانه‌های زیست‌سنجی، مربوط به خطر افتادن مراجع زیست‌سنجی است. انواع مختلفی از تهدیدات می‌تواند یک مرجع زیست‌سنجی را به خطر بیندازد. به عنوان مثال، ممکن است یک مهاجم بطور غیرقانونی یک نشانه حاوی یک مرجع زیست‌سنجی را بدست آورده، یا ممکن است تلاش کند با استفاده از یک زیست‌سنجه تقلبی یا جعلی، یک دسترسی غیرمجاز از طریق پذیرش اشتباه[3] به‌دست آورد. در هنگام به‌خطر افتادن، برای جلوگیری از دسترسی غیر مجاز مهاجم در آینده (و یا ادامه دادن به آن)، ابطال ضروری است. از طرف دیگر، یک رخنه امنیتی در پایگاه داده ممکن است منجر به افشای غیرمجاز مراجع زیست‌سنجی و دیگر داده‌های شخصی گردد. در شرایطی که مراجع زیست‌سنجی اینگونه به خطر بیفتند، قویا نیاز به فسخ مراجع به‌خطر افتاده، انتساب موضوع داده قانونی با یک مرجع زیست‌سنجی جدید داریم. باید توجه داشت که برای فسخ و تجدید مرجع زیست‌سنجی، لزومی بر تجدید مشخصه‌های زیست‌سنجی موضوع داده نمی‌باشد. تجدیدپذیری و ابطال‌پذیری فقط ابزاری برای حل مشکل مراجع زیست‌سنجی به خطرافتاده ارائه می‌نماید، و مسئله مشخصه‌های زیست‌سنجی به خطر افتاده را برطرف نمی‌کند.

ممکن است یک مرجع زیست‌سنجی به دلایل مختلف دیگری، علاوه‌بر به خطر افتادن، نیاز به تغییرداشته باشد. به عنوان مثال، ممکن است یک مرجع زیست‌سنجی تنها برای دوره زمانی خاصی معتبر باشد (به روشی مشابه کلمات

1 -replay attack
2 -Message authentication code
3 -false accept

عبور). اگر در پایان این دوره زمانی، هنوز هم به مرجع زیست‌سنجی نیاز باشد، آن مرجع مجاز است تجدید شده، یا ابتدا فسخ و سپس جایگزین گردد.

۵-۲ تهدیدات امنیتی و اقدامات متقابل در سامانه زیست‌سنجی

۵-۲-۱ تهدیدات و اقدامات متقابل در برابر مولفه‌های سامانه‌های زیست‌سنجی

تهدیدات علیه مولفه‌های یک سامانه زیست‌سنجی در جدول ۱ خلاصه شده است [۸].

جدول ۱ - تهدیدات و اقدامات متقابل زیرسامانه‌های زیست‌سنجی

	تهدیدات	اقدامات متقابل
اخذ داده	کلاه برداری حسگر اخذ / پاسخ سیگنالهای حسگر	تشخیص زندگی زیست سنجی چندحالته چالش / پاسخ
پردازش سیگنال	دستکاری غیرمجاز داده هنگام پردازش	استفاده از الگوریتم مورد اعتماد
مقایسه	دستکاری امتیازهای مقایسه	کارسازکارساز و یا مشتری امن OCC مورد اعتماد
ذخیره سازی	مقایسه پایگاه داده افشای غیرمجاز IR/BR جایگزینی غیرمجازIR/BR تغییر غیرمجازIR/BR حذف غیرمجازIR/BR	مراجع زیست سنجی ابطال پذیر و تجدیدپذیر جداسازی داده کنترل دسترسی پایگاه داده امضای BR/RBR/IR رمزگذاری BR/RBR/IR
تصمیم	حمله تپه نوردی	کانال امن اختفای امتیاز مقایسه از موضوع
	دستکاری آستانه	کنترل دسترسی به تنظیمات آستانه محافظت مقدار آستانه

یادآوری ۱- برای کسب اطلاعات بیشتر در مورد ارزیابی و صدور گواهینامه[1] امن مولفه‌های پیمانه‌ای سامانه‌های زیست‌سنجی، به ISO/IEC 19792 مراجعه نمایید.

یادآوری ۲- پیاده سازی مولفه‌های مقایسه و تصمیم گیری در یک پیمانه واحد تصدیق شده[2] متشکل از یک اقدام متقابل موثر در برابر تهدیدات دستکاری امتیازمقایسه[3] است. در اینجا، برای جلوگیری از حمله تپه نوردی[4]، نیاز به یک اقدام متقابل اضافی برای مخفی کردن امتیاز از موضوع می‌باشد.

یادآوری ۳- تهدید جایگزینی مولفه۵ در همه زیر سامانه‌ها کاربست‌پذیر است. استفاده از کنترل فهرست موجودی ازجمله مولفه‌هایی که امضای رقمی شده‌اند، می‌تواند اقدام متقابل موثری برای مقابله با این تهدید باشد.

برای روشن شدن موضوع، شرح خلاصه ای از تهدیدات اشاره شده در بالا و اقدامات متقابل در زیر ارائه شده است.

- جعل حسگر به معنای ارائه مصنوعی، و در نتیجه غیر زنده مشخصه‌های زیست‌سنجی است. یک اقدام متقابل برای جعل حسگر، کشف زنده بودن براساس بازشناسی فعالیت‌های فیزیولوژیکی یک موضوع به عنوان علائمی از زندگی، و یا کشف و سپس رد انواع خصوصیات مصنوعی شناخته‌شده می‌باشد.

- جایگزینی مولفه شامل جایگزینی مولفه‌های (به عنوان مثال، زیرسامانه مقایسه یا تصمیم گیری) سامانه زیست‌سنجی، به‌منظور کنترل آن و به‌دست آوردن خروجی موردنظر می‌باشد.

- تپه نوردی، به‌معنای تغییر نظام‌مند نمونه زیست‌سنجی برای به دست آوردن امتیازهای مقایسه بالاتر به‌صورت تصاعدی است، تا زمانی‌که حد آستانه تصمیم‌گیری برآورده شود.

- دستکاری آستانه[6]، به‌معنای تغییر مقدار آستانه زیرسامانه تصمیم گیری است به‌طوری که سامانه زیست‌سنجی به راحتی نمونه‌های زیست‌سنجی غیرمجاز را بپذیرد.

- مراجع زیست‌سنجی ابطال‌پذیر و تجدیدپذیر با استفاده از روش متنوع‌سازی[1] برای برنامه‌های کاربردی، سازمان‌ها یا شرکت‌های مختلف ایجاد می‌شوند، اما همگی آن‌ها به موضوع یکسانی منتسب می‌گردند. موضوعات مجاز هستند که چندین RBR داشته باشند.

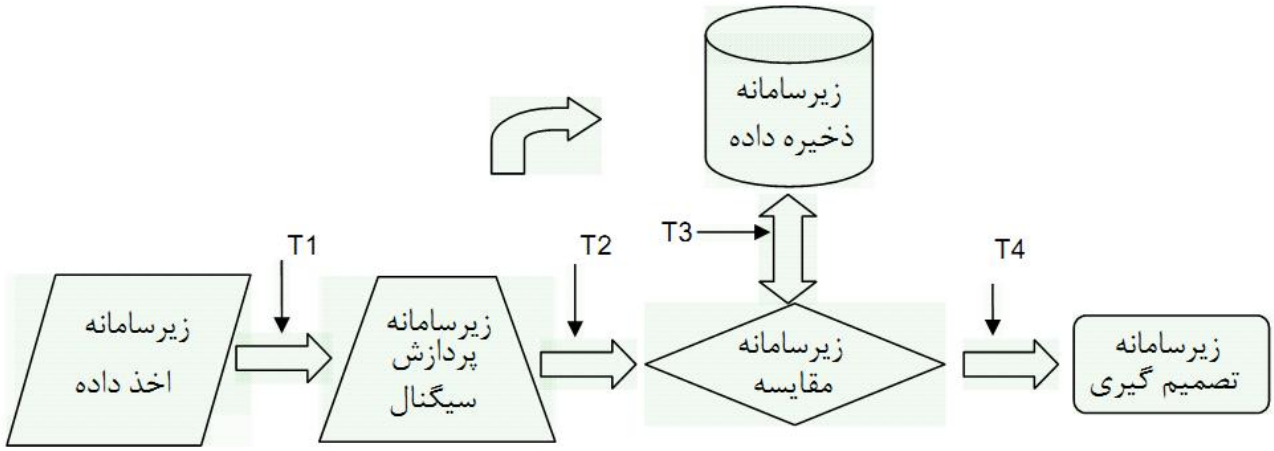
---

[1] Certification
[2] Certified single module
[3] Comparison score manipulation
[4] Hill climbing
5-Component replacement
6-Threshold manipulation

- منظور از جداسازی داده‌ها، اقدام متقابل امنیتی برای جداسازی منطقی یا فیزیکی عناصر داده منفرد می‌باشد (به عنوان مثال بخشی روی نشانه و بخشی دیگر در یک پایگاه داده قرار گیرند، همچنین بند ۷.۲ را ببینید) می‌باشد. جداسازی داده‌ها می‌تواند روی عناصر داده‌ای مانند IR، BR، PI و AD اعمال شود.

۵-۲-۲ تهدیدات و اقدامات متقابل هنگام انتقال اطلاعات زیست‌سنجی

ممکن است کانال‌های ارتباطی بین مولفه‌های مختلف سامانه زیست‌سنجی به خطر افتاده و امنیت کل سامانه را به خظر بیندازند. این خطر مخصوصا معماری‌های توزیع شده را تهدید می‌کند. رخدادهای انتقال اطلاعات در شکل ۴ نشان داده شده و در جدول ۲ خلاصه شده‌اند. در جدول ۲، اگر یک شبکه بین زیرسامانه‌های مقایسه و تصمیم گیری قرار گیرد، مخاطرات و اقدامات متقابلشان برای T1، T2 و T3 برای T4 نیز قابل اعمال است.



شکل ۴ – مخاطرات سامانه زیست‌سنجی

جدول ۲ – مخاطرات و اقدامات متقابل هنگام انتقال

	داده	تهدیدات	اقدامات متقابل
ضبط داده – پردازش سیگنال (T1)	ویژگی و نمونه زیست سنجی	استراق سمع	کانال امن/ رمزگذاری شده
		پخش	چالش / پاسخ

1 -Diversification

پردازش سیگنال – مقایسه (T2)		۵-۲-۳ گسترده [1]	سیاست پایان زمان
ذخیره – مقایسه (T3)	مرجع زیست سنجی	استراق سمع	کانال امن / رمزگذاری شده
		پخش	چالش / پاسخ
		۵-۲-۴ مردی –در- میان [2]	کانال امن / رمزگذاری شده بررسی تمامیت داده زیست سنجی با امضای دیجیتال یا MAC
		تپه نوردی	امتیازهای ؟!؟!؟(Coarse) کانال امن
مقایسه – تصمیم (T4)	امتیاز مقایسه	تغییر امتیاز مقایسه	کانال امن

1-Brute Force

۲-Man in the middle

یادآوری- پیاده‌سازی مولفه‌های مقایسه و تصمیم گیری در یک ماژول واحد تصدیق‌شده[1] به منزله یک اقدام متقابل موثر در مقابل تهدیدات دستکاری امتیاز مقایسه می‌باشد

برای روشن شدن موضوع، شرح خلاصه ای از تهدیدات اشاره شده در بالا در زیر بیان شده است:

- استراق سمع، به‌معنای رهگیری اطلاعات حساس، در زمان انتقال بین مولفه‌های سامانه زیست‌سنجی است.

- حملات مردی-در-میان[2] حملاتی هستند که در آن‌ها حمله کننده قادر به خواندن، درج و تغییر داده‌های زیست‌سنجی مبادله‌شده بین دو طرف می‌باشد، بدون اینکه هیچیک از طرفین بداند که پیوند برقرارشده به خطر افتاده است.

فهرست اقدامات متقابل در جدول ۲ جامع نیست. برای شناسایی تهدیدات در بافت برنامه کاربردی بهتر است ابتدا تحلیل خطر انجام شود. سپس اقدامات متقابل مناسب، که می‌تواند شامل اقدامات متقابل رویه‌ای و فنی باشد، انجام پذیرد. برای دیدن توصیف جزئی‌تری از جنبه‌های مدیریتی حفاظت از سامانه‌های زیست‌سنجی به ITU-T X.1086 [1]، ،[2] ISO 19092:2008 وISO/IEC 19792 ،[۴۳]مراجعه شود.

[1] Certified

2 -Man-in-the-middle

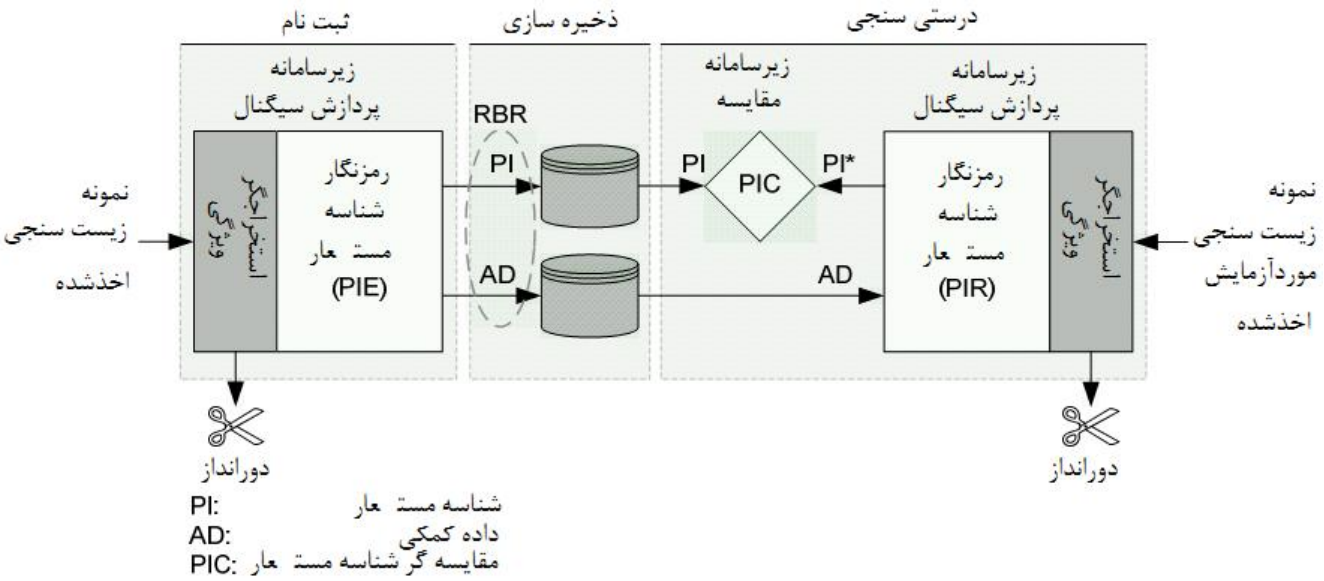
۵-۲-۵ مراجع تجدیدپذیر زیست‌سنجی به‌عنوان فناوری اقدامات متقابل

تجدیدپذیری مراجع زیست‌سنجی یک اقدام متقابل در برابر تهدیدهای ذخیره سازی و انتقال است. برای اینکه فسخ یا تجدید مراجع زیست‌سنجی مجاز باشد، بهتر است فرآیند ایجاد مراجع زیست‌سنجی از فرآیند متنوع‌سازی پشتیبانی کند. متنوع‌سازی عبارتست از ایجاد مراجع متعدد و مستقل از مشخصه‌های زیست‌سنجی یکسان که می‌تواند برای تجدید یک مرجع زیست‌سنجی، یا تهیه مراجع مستقل در بین برنامه‌های کاربردی مختلف مورد استفاده قرار گیرد. بهتر است فرآیند متنوع‌سازی برگشت‌ناپذیر باشد. مراجع زیست‌سنجی تبدیل‌شده نباید به‌صورت یکتا پیوندپذیر باشند.

برای کمک به ایجاد یک فرهنگ واژگان مشترک برای پیاده‌سازی مراجع تجدید پذیر زیست‌سنجی (RBRs) از طریق یک فرآیند متنوع‌سازی، و برای طرح جنبه‌های معماری مراجع تجدید پذیر زیست‌سنجی و فرآیند متنوع‌سازی به یک شیوه مستقل از فناوری، مفهوم شناساگرهای مستعار در این استاندارد ملی مورد استفاده قرار می‌گیرد. در روش شرح داده شده در این استاندارد ملی، منابع تجدیدپذیر زیست‌سنجی از دو عنصر داده تشکیل می‌گردد: یک شناساگر مستعار (PI) و داده‌های کمکی متناظر با آن (AD). ازآنجایی که هر دو عنصر در طی یک فرآیند درستی‌سنجی یا شناسایی موردنیاز هستند، هر دو عنصر داده هنگام ثبت‌نام تولید شده و باید ذخیره شوند.

یک دیدگاه کلی از جنبه‌های معماری مراجع تجدید پذیر زیست‌سنجی در شکل ۵ ارائه شده است. در این شکل، یک پیکان نشان‌دهنده جریان اطلاعات است. در هنگام ثبت نام، داده‌های ویژگی زیست‌سنجی به‌وسیله یک مرحله استخراج ویژگی، از نمونه زیست‌سنجی اخذشده تولید می‌شوند. در ادامه، یک مرجع تجدید پذیر زیست‌سنجی متشکل از یک شناساگر مستعار (PI) و داده‌های کمکی (AD) به‌وسیله یک کدبندی‌کننده شناساگرمستعار (PIE)، تولید می‌شود. هنگامی‌که RBR ایجاد می‌شود، نمونه زیست‌سنجی اخذ شده و ویژگی‌های استخراج شده می‌توانند به‌صورت امن، نابود شوند. RBR بر روی یک رسانه ذخیره سازی مناسب (به عنوان مثال، یک کارت هوشمند یا پایگاه داده الکترونیکی) ذخیره می‌شود. PI و AD مجاز هستند که به‌صورت فیزیکی یا منطقی از یکدیگر جدا شوند .

در هنگام درستی‌سنجی، یک مرحله استخراج ویژگی، نمونه زیست‌سنجی موردآزمایش را پردازش می‌کند. سپس، بر اساس داده‌های کمکی ارائه شده و ویژگی‌های استخراج شده، یک شناساگر مستعار (*PI) به‌وسیله یک ضبط کننده شناساگر مستعار (PIR)ساخته می‌شود. پس از آن، زیرسامانه مقایسه PI تولید شده هنگام ثبت نام و*PI را مقایسه کرده و یک امتیاز شباهت که نشان‌دهنده میزان شباهت میان PI و *PI است را برمی‌گرداند. بررسی گسترده‌تر فرآیندهای ایجاد و درستی‌سنجی شناساگر مستعار، به‌همراه چرخه عمر آن، در ضمیمه پ آورده شده است.



شکل ۵- معماری مراجع زیست‌سنجی تجدیدپذیر

داخل شکل (رمزنگار به رمز گذار تغییر نماید)

۵-۳ امنیت رکوردهای داده حاوی اطلاعات زیست‌سنجی

۵-۳-۱ امنیت برای پردازش اطلاعات زیست‌سنجی در یک دادگان واحد

همانطور که در شکل ۱ نشان داده شده است، برای انجام عملیات احراز هویت زیست‌سنجی، نیاز به الحاق منطقی یک هویت مرجع (IR) با یک مرجع زیست‌سنجی (BR) می‌باشد. چندین سناریوی کاربست‌پذیر موجود است که بسته به رکوردهای داده‌ای (به عنوان مثال، هویت مرجع، مرجع زیست‌سنجی، و غیره) که ذخیره شده‌اند، می‌توانند برای توصیف امنیت این انقیاد، مورد استفاده قرار گیرند. این سناریوها که نشاندهنده ترکیبات عناصر داده‌ای، به‌همراه خواص امنیتی مربوطه می‌باشند، در زیر فهرست می‌شوند.

- **سناریوی۱:** IR خام و BR خام ذخیره می‌شوند. نه محرمانگی و نه یکپارچگی برای IR و BR تأمین نمی‌شود. تجدیدپذیری و ابطال‌پذیری نیز تأمین نمی‌شوند.

- **سناریوی ۲:** IR خام و BR رمزگذاری شده ذخیره می‌شوند. نه محرمانگی و نه یکپارچگی در IR فراهم نمی‌شوند. محرمانگی برای BR تامین می‌شود. بسته به حالت عملیات رمزگذاری ممکن است شکل ضعیفی از یکپارچگی برای BR ارائه شود. تجدیدپذیری و ابطال‌پذیری تامین نمی‌شود.

- **سناریوی ۳:** IR خام و BR احراز هویت شده ذخیره می‌شوند. فقط یکپارچگی برایBR تامین می‌شود.

- **سناریوی ۴:** IR خام و شکل احرازهویت-رمزگذاری شده BR ذخیره می‌شود. هم محرمانگی و هم یکپارچگی برای BR تامین می‌شوند.

- **سناریوی ۵:** IR رمز شده و BR خام ذخیره می‌شوند. محرمانگی برای IR تامین می‌شود.ممکن است بسته به حالت عملیات رمزگذاری، شکل ضعیفی از یکپارچگی برای IR تامین گردد.

- **سناریوی ۶:** IR احراز هویت شده و BR خام ذخیره می‌شوند. یکپارچگی فقط برای IR تامین می‌گردد.

- **سناریوی ۷:** شکل احراز هویت-رمزگذاری شده IR و BR خام ذخیره می‌شوند. محرمانگی و یکپارچگی فقط برای IR تامین می‌گردند.

- **سناریوی ۸:** IR و BR خام رمزگذاری شده و پس از آن ذخیره می‌شوند. محرمانگی برای هر دوی IR و BR تامین می‌شود. ممکن است بسته به حالت عملیات رمزگذاری، شکل ضعیفی از یکپارچگی برای هر دوی IR و BR، تامین گردد.

- **سناریوی ۹:** IR خام و BR خام، احراز هویت شده و سپس ذخیره می‌شوند. یکپارچگی برای هر دوی IR و BR تامین می‌گردد.

- **سناریوی ۱۰:** اشکال احرازهویت- رمز گذاری شده IR و BR ذخیره می‌شوند. محرمانگی و یکپارچگی برای هر دوی IR و BR تامین می‌گردد.

- **سناریوی ۱۱:** IR خام و BR احرازهویت شده، رمزگذاری و سپس ذخیره می‌شوند. محرمانگی برای هر دوی IR و BR تامین می‌شود. یکپارچگی برای BR تامین می‌شود. ممکن است بسته به حالت عملیات رمزگذاری، شکل ضعیفی از یکپارچگی برای IR تامین شود.

- **سناریوی۱۲:** IR خام و BR رمزگذاری شده، احراز هویت شده و بعد ذخیره می‌شوند. یکپارچگی برای هر دوی IR و BR تامین می‌شود. محرمانگی تنها برای BR تامین می‌شود.

- **سناریوی ۱۳:** IR احراز هویت شده و BR خام، رمزگذاری شده و بعد ذخیره می‌شوند. محرمانگی برای هر دوی IR و BR تامین می‌گردد. یکپارچگی برای IR تامین می‌شود. ممکن است بسته به حالت

عملیات الگوریتم رمزگذاری زیرین، شکل ضعیفی از یکپارچگی برای BR تامین شود.

- **سناریوی ۱۴:** IR رمزگذاری شده و BR خام، احراز هویت شده، و سپس ذخیره می‌شوند. یکپارچگی در هر دوی IR و BR تامین می‌شود. محرمانگی فقط برای IR تامین می‌گردد.

- **سناریوی ۱۵:** IR خام و BR متنوع‌شده[1] ذخیره می‌شوند. تجدیدپذیری و ابطال‌پذیری برای BR تامین می‌شوند، همچنین یکپارچگی و محرمانگی به‌طور محدود برای BR تامین می‌شوند.

- **سناریوی ۱۶:** IR خام و BR متنوع‌شده احراز هویت شده و بعد ذخیره می‌شوند. یکپارچگی برای هر دوی IR و BR تامین می‌شود. همچنین تجدیدپذیری و ابطال‌پذیری برای BR تامین می‌شود.

- **سناریوی ۱۷:** اشکال احرازهویت-رمزگذاری شده IR و متنوع‌شده BR ذخیره می‌شوند. یکپارچگی و محرمانگی در هر دوی IR و BR تامین می‌شود. تجدیدپذیری و ابطال‌پذیری برای BR تامین می‌شود.

- **سناریوی ۱۸:** IR خام و BR متنوع‌شده، رمزگذاری و بعد ذخیره می‌شوند. محرمانگی برای هردوی IR و BR تامین می‌شود. ممکن است بسته به حالت عملیات، شکل ضعیفی از یکپارچگی برای هردوی IR و BR تامین شود. تجدیدپذیری و ابطال‌پذیری برای BR تامین می‌شود.

- **سناریوی ۱۹:** IR خام و BR رمزگذاری و متنوع شده، احرازهویت شده و سپس ذخیره می‌شوند. یکپارچگی برای هردوی IR و BR تامین می‌شود. محرمانگی، تجدیدپذیری و ابطال‌پذیری فقط برای BR تامین می‌شود.

سناریوهای شرح داده شده و ملاحظات امنیتی مربوطه در جدول ۳ خلاصه شده است.

1 -Diversified

جدول ۳: محرمانگی، یکپارچگی و تجدیدپذیری برای رکوردهای اطلاعاتی ذخیره شده در یک پایگاه داده واحد

(O:الزامات،Δ:الزامات ضعیف)

سناریو	الزامات امنیتی					اقدامات متقابل
	محرمانگی		یکپارچگی		تجدیدپذیری	
	IR	BR	IR	BR	BR	
۲		0		Δ		IR خام و BR رمزشده
۳				0		IR خام و BR تصدیق شده
۴		0		0		IR خام و BR تصدیق-رمز شده
۵	0		Δ			IR رمزشده و BR خام
۶			0			IR تصدیق شده و BR خام
۷	0		0			IR تصدیق-رمز شده و BR خام
۸	0	0	Δ	Δ		(IR و BR) رمزشده
۹			0	0		(IR و BR) تصدیق شده
۱۰	0	0	0	0		(IR و BR) تصدیق -رمزشده
۱۱	0	0	Δ	0		(IR و BR تصدیق شده) رمز شده
۱۲		0	0	0		(IR و BR رمز شده) تصدیق شده
۱۳	0	0	0	Δ		(IR تصدیق شده و BR) رمزشده
۱۴	0		0	0		(IR رمز شده و BR) تصدیق شده
۱۵					0	IR خام و BR متنوع
۱۶		Δ	0	0	0	(IR و BR متنوع) تصدیق-رمز شده
۱۷	0	0	0	0	0	(IR و BR متنوع) تصدیق-رمز شده
۱۸	0	0	Δ	Δ	0	(IR و BR متنوع) رمزشده
۱۹		0	0	0	0	(IR و BR رمزشده متنوع) تصدیق شده

ISO/IEC 19785، با تعیین یک ساختار استاندارد برای رکوردهای اطلاعات زیست‌سنجی (BIRs[1])، چارچوب قالب تبادل زیست‌سنجی مشترک (CBEFF[2]) را برای ارتقا قابلیت همکاری برنامه‌های کاربردی و

1 -Biometric Information Record
2 -Common Biometric Exchange Format Framework

سامانه‌های مبتنی بر زیست‌سنجی، مشخص می‌کند. در ISO/IEC 19785-4 ، قالب‌های قطعه امنیتی (SB[1]) برای حفظ یکپارچگی BIRs و رمزگذاری/رمزگشایی داده‌های زیست‌سنجی در BIRs مشخص شده‌اند[۳].

۵-۳-۲ امنیت برای پردازش اطلاعات زیست‌سنجی در پایگاه داده‌های مجزا

اگر حفظ حریم خصوصی الزامی است، توصیه می‌شود در هنگام ذخیره سازی IR و BR یا RBR، آن‌ها را به‌طور جداگانه ذخیره نمایید، چراکه افشای همزمان هر دو قسمت باعث به خطر افتادن جدی‌تر حریم خصوصی می‌گردد. حتی اگر IR و BR به‌صورت مجزا، در ناحیه‌های ذخیره‌سازی متفاوت قرار گرفته باشند، چنانچه به‌وسیله متصدی یکسانی کنترل گردند، حفاظت موثر نخواهد بود. برای اینکه جداسازی موثر باشد، بهتر است این دو به‌وسیله متصدیان مختلفی کنترل گردند، که هریک کلیدهای رمزگذاری مختص به خودشان را برای حفاظت از محتویات پایگاه داده خود دارند. هنگامیکه IRو BR از هم جدا می‌شوند، باید وسیله ای برای پیوند آن‌ها وجود داشته باشد. این مسئله به‌وسیله یک شناساگر مشترک، CI، حاصل می‌شود.

استدلال مشابهی برای ذخیره سازی RBRs در قالب PI و AD برقرار است. جداسازی فیزیکی یا منطقی PI و AD مخاطرات حفظ حریم خصوصی و امنیتی را کاهش می‌دهد. جدایی فیزیکی مطلوب است. اگر نشانه‌ها در یک مدل مبتنی بر ذخیره‌سازی توزیع‌شده بکار گرفته شوند، توصیه می‌شود AD روی نشانه، و PI بر روی مشتری یا کارساز ذخیره شوند. اگر پایگاه داده‌های مجزا با یک CI مشترک، بکار گرفته شوند، پایگاه‌های داده باید به‌وسیله متصدیان جداگانه، با کلیدهای رمزگذاری مختلف کنترل شوند. در جدول ۴، سناریوهای به کارگیری پایگاه داده‌های مجزا نشان داده شده است. الزامات امنیتی محرمانگی، یکپارچگی، و تجدیدپذیری/ ابطال‌پذیری به همان شکل باقی می‌مانند. با این وجود، اگر تنها یکی از IR و BR افشا شوند، تاثیر به خطرافتادن حریم خصوصی کمتر می‌شود. اگر یک DB به خطر بیافتد و محتویات آن به صورت غیرقانونی تغییر کند، متصدیان این دو DB باید قادر به کشف آن باشند. به طور مشابه، در هنگام استفاده از DBها، اگر یک متصدی DB قانونی با یک کلید درست، محتوای آن را تغییر دهد، DB دیگر باید قادر به کشف آن تغییر باشد. برای چنین مواردی، به انقیاد امن‌تری نیاز است. ضمیمه الف نمونه‌هایی از پیاده‌سازی یک شناساگر مشترک (CI) را ارائه می‌کند.

1 -Security Block

جدول ۴ – محرمانگی، یکپارچگی و تجدیدپذیری برای رکوردهای داده ذخیره‌شده در پایگاه داده‌های مجزا

(O:الزامات،Δ:الزامات ضعیف)

اقدامات متقابل برای BR	اقدامات متقابل برای IR	الزامات امنیتی				
		تجدید پذیری	یکپارچگی		محرمانگی	
		BR	BR	IR	BR	IR
CI و BR رمزشده	CI و IR خام		Δ		o	
CI و BR تصدیق شده	CI و IR خام		o			
CI و BR تصدیق-رمز شده	CI و IR خام		o		o	
CI و BR خام	CI و IR رمزشده					o
CI و BR خام	CI و IR تصدیق شده			o		
CI و BR خام	CI و IR تصدیق-رمز شده			o		o
CI و BR رمزشده	CI و IR رمزشده		Δ	Δ	o	o
CI و BR تصدیق شده	CI و IR تصدیق شده		o	o		
CI و BR تصدیق-رمز شده	CI و IR تصدیق-رمز شده		o	o	o	o
CI و BR تصدیق-رمز شده	CI و IR رمزشده		o	Δ	o	o
CI و BR تصدیق-رمز شده	CI و IR تصدیق شده		o	o	o	
CI و BR رمزشده	CI و IR تصدیق-رمز شده		Δ	o	o	o
CI و BR تصدیق شده	CI و IR تصدیق-رمز شده		o	o		o
CI و AD	CI و PI و IR	o			Δ	
CI و AD تصدیق شده	CI و PI تصدیق شده و IR تصدیق شده	o	o	o	Δ	
CI و AD تصدیق-رمز شده	CI و (PI و IR) تصدیق-رمز شده	o	o	o	o	o
CI و AD رمز شده	CI و (PI و AR) رمز شده	o	Δ	Δ	o	o
CI و (AD رمزشده) تصدیق شده	CI و (PI رمزشده و IR) تصدیق شده	o	o	o	o	o

۶ مدیریت حفظ حریم خصوصی اطلاعات زیست‌سنجی

۶-۱ تهدیدات حفظ حریم خصوصی اطلاعات زیست‌سنجی

از آنجا که داده‌های زیست‌سنجی (از نوع PII) هستند، بهتر است استاندارد IEC/ISO29100 در مورد آن‌ها اعمال گردد که یک چارچوب حفظ حریم خصوصی کلی است که مسائل مختص به سامانه را به‌صورت سطح

بالا نشان می‌دهد.(جمله‌ی های لایت شده اصلاح شود) این استاندارد یک چارچوب کلی است که جنبه‌های سازمانی، فنی، رویه‌ای و تنظیم مقررات حفظ حریم خصوصی سامانه‌های IT را که اطلاعات شخصی را پردازش و ذخیره می‌نمایند، نشان می‌دهد. استفاده از اطلاعات زیست‌سنجی دربرگیرنده تهدیدات متعددی برای حفظ حریم خصوصی است که باید مورد توجه قرار گیرند.

- ممکن است داده‌های زیست‌سنجی برای مقاصدی غیر از آنچه در اصل مورد نظر و رضایت موضوع بوده، مورد سوءاستفاده قرار گیرند.
- ممکن است مراجع زیست‌سنجی امکان بازیابی و یا تحلیل خاصیت‌هایی از موضوع داده را بدهد که برای شناسایی و درستی‌سنجی مبتنی بر زیست‌سنجی موردنیاز یا موردنظر نبوده‌اند، مانند وضعیت سلامت موضوع داده و یا اطلاعات پزشکی استنباطی و پیش‌زمینه نژادی.
- ممکن است مراجع زیست‌سنجی برای پیوند موضوعات میان برنامه‌های کاربردی مختلف در یک پایگاه داده یکسان، و یا میان پایگاه‌داده‌های متفاوت استفاده شوند. حفظ حریم خصوصی به‌معنای پیوندناپذیری مرجع زیست‌سنجی ذخیره شده است.

توصیف با جزئیات بیشتر ملاحظات اداری و قضایی و اجتماعی برای کاربرد تجاری زیست‌سنجی در استاندارد ISO/IEC TR 24714-1 [۱۹] شرح داده می‌شود.

۶-۲ الزامات حفظ حریم خصوصی اطلاعات زیست‌سنجی و راهنمایی‌ها

۶-۲-۱ بازگشت‌ناپذیری

برای جلوگیری از به‌کاربردن اطلاعات زیست‌سنجی برای مقاصد دیگری به‌جز آنچه در اصل در نظر گرفته شده است، داده‌های زیست‌سنجی باید پیش از ذخیره سازی، به‌وسیله مبدل‌های بازگشت‌ناپذیر پردازش شوند. بازگشت‌ناپذیری می‌تواند به‌وسیله سازوکارهای زیر، که امکان ترکیب آن‌ها نیز وجود دارد، حاصل گردد:

- الگوریتم‌های استخراج ویژگی، اغلب شکلی از بازگشت‌ناپذیری را با استفاده از کاهش داده‌ها و حذف افزونگی ارائه می‌کنند، که باعث سخت‌تر شدن استفاده از ویژگی‌های استخراج شده برای استخراج داده‌های پزشکی و یا نژادی می‌گردد.

- رمزگذاری با استفاده از کلیدی که فقط در اختیار متصدی سامانه و/یا موضوع داده باشد، دسترسی غیرمجاز به داده‌های زیست‌سنجی را محدود می‌سازد؛

- شناساگرهای مستعار ابزاری برای محدود کردن دسترسی به مشخصه‌های زیست‌سنجی موضوع داده، با

استفاده از تبدیلات بازگشت‌ناپذیر، فراهم می‌آورند. مروری کلی بر تبدیلاتی که شناساگرهای مستعار را تولید می‌نماید در پیوست ت ، جدول ت.۱ ارائه شده است.

۶-۲-۲ پیوندناپذیری

توصیه می‌شود مراجع زیست‌سنجی ذخیره شده در بین برنامه‌های کاربردی و یا دادگان‌ها، پیوندپذیر نباشند. پیوندناپذیری را می‌توان با استفاده از سازوکارهای مختلفی که قابل ترکیب نیز می‌باشند، فراهم کرد :

- اگر مراجع زیست‌سنجی متن-اولیه[1] پیوندپذیر هستند، آنگاه رمزگذاری مراجع زیست‌سنجی با استفاده از کلیدها (سری) یا سازوکارهای متفاوت در بین برنامه‌های کاربردی، مانع از پیوند موضوعات داده می‌شود؛ البته به‌شرطی‌که کلیدهای سری برای جلوگیری از تداخل، به‌طور مناسبی مدیریت گردند(نقطه ویرگول)

- شناساگرهای مستعار مستقل و پیوندناپذیر ایجاد شده از طریق فرآیند متنوع‌سازی، مانع از پیوند موضوعات داده می‌شوند؛

- جداسازی منطقی یا فیزیکی IR و BR، یا PI و AD در مورد RBRها، مانع از دسترسی به رکوردهای داده کامل می‌شود.؛

- استفاده از روش‌های مختلف زیست‌سنجی، و الگوریتم‌های استخراج ویژگی یا قالب‌های تبادل داده زیست‌سنجی ناسازگار در بین برنامه‌های کاربردی، مانع از پیوند موضوعات داده می‌شود.

یادآوری- استفاده از روش‌های مختلف زیست‌سنجی، و الگوریتم‌های استخراج ویژگی یا قالب‌های تبادل داده ناسازگار ممکن است چالش‌هایی برای قابلیت همکاری سامانه در بر داشته باشد.

۶-۲-۳ محرمانگی

برای محافظت از منابع زیست‌سنجی در مقابل دسترسی به‌وسیله یک هستار غیر مجاز و در نتیجه به خطر افتادن حفظ حریم خصوصی، مراجع زیست‌سنجی باید محرمانه باقی بمانند. سازوکارهای زیر را می‌توان برای تأمین محرمانگی به کار برد:

1-Plain-text

- یک اقدام متقابل به منظور کاهش مخاطرات حفظ حریم خصوصی ناشی از یک نقص امنیتی در پایگاه داده متمرکز (به عنوان مثال وقتی که یک رقیب، دسترسی غیرقانونی به دادگان متمرکز بدست آورده و محتویات آن را منتشر می‌کند)، تفکیک داده‌ها به‌وسیله ذخیره‌سازی (بخشی از) مراجع زیست‌سنجی بر روی یک نشانه یا کارت شخصی، به جای استفاده از دادگان‌های متمرکز می‌باشد ؛

- رمزگذاری مراجع زیست‌سنجی با استفاده از یک کلید که فقط در اختیار متصدی سامانه مدیریت هویت و/یا موضوع داده می‌باشد.

یادآوری- استفاده از یک نشانه برای ذخیره داده‌های زیست‌سنجی، محرمانگی را تضمین نمی‌کند، مگر اینکه داده‌ها بصورت منطقی و فیزیکی در مقابل افشا محافظت شده باشند.

۶-۳ الزامات قانونی و خط‌مشی

جمع آوری، انتقال، استفاده، ذخیره و از بین بردن یک مرجع زیست‌سنجی، به عنوان یک PII، تحت قوانین و مقررات مختلفی، از جمله حفظ حریم خصوصی و محافظت از داده‌ها، مدیریت می‌شود. تمام استقرارهای فناوری زیست‌سنجی باید مطابق با تمام قوانین و مقررات کاربست‌پذیر، پیاده‌سازی گردد.

۶-۴ مدیریت حفظ حریم خصوصی چرخه عمر اطلاعات زیست‌سنجی

۶-۴-۱ جمع آوری[1]

سازمان‌ها باید قبل ازجمع آوری اطلاعات زیست‌سنجی رضایت موضوع را کسب کنند، مگر اینکه قوانین و مقررات قابل‌کاربرد، تعریفی غیر از این داشته باشند. توصیه می‌شود سازمان در هنگام کسب رضایت موضوع، موارد زیر را به‌طور کامل به اطلاع وی برساند (توجه کنید که این فهرست جامع نیست):

- انواع و مقدار اطلاعات زیست‌سنجی که اخذ می‌گردد؛

- اطلاعاتی در مورد رویّه‌های جایگزین موجود، در مواردی که موضوع داده تمایلی به ثبت‌نام نداشته باشد و یا نتواند ثبت‌نام کند (عدم موفقیت در ثبت‌نام)؛

- هدف از جمع آوری و دوره نگهداری اطلاعات زیست‌سنجی؛

1-Collection

- توصیفی از نحوه پردازش اطلاعات زیست‌سنجی اخذشده در سامانه زیست‌سنجی؛ و

- اطلاعاتی راجع به فرد مسئول مدیریت اطلاعات زیست‌سنجی،که شامل نام، سازمان، موقعیت، اطلاعات تماس، و غیره می‌باشد.

جمع‌آوری غیرمجاز اطلاعات زیست‌سنجی بدون هیچگونه توجیه قانونی، اثرات شدیدی بر حفظ حریم خصوصی اطلاعات زیست‌سنجی فرد دارد. با وجود اینکه ممکن است یک سازمان رضایت موضوع را برای ایجاد مراجع زیست‌سنجی داشته باشد، هنوز هم بهتر است کمینه میزان اطلاعات زیست‌سنجی لازم برای تحقق اهداف مورد نظر را استخراج نماید. این کار تأثیر به خطرافتادن را کاهش خواهد داد.

۶-۴-۲ انتقال (افشای[1] اطلاعات به طرف سوم)

هنگام انتقال اطلاعات زیست‌سنجی به سازمان‌های دیگر، هر یک از طرفین درگیر در پردازش اطلاعات زیست‌سنجی باید موافقت نمایند که از طریق یک قرارداد یا تعهد، ملزم به محافظت از آن اطلاعات گردند. انتقال اطلاعات زیست‌سنجی فقط باید با رضایت موضوع صورت پذیرد، مگر اینکه ارائه خدمت درخواست‌شده به‌وسیله موضوع، دلالت ضمنی بر رضایت وی داشته باشد، و یا براساس قانون موردنیاز باشد.
قبل از آنکه سازمان بدنبال رضایت موضوع باشد، بهتر است موارد زیر را فراهم کند (توجه داشته باشید که این فهرست جامع نیست):

- اطلاعات مربوط به طرف سومی که اطلاعات زیست‌سنجی به او منتقل می‌شود؛

- محتویات و میزان اطلاعات زیست‌سنجی که منتقل می‌شود و

- هدف از انتقال و دوره نگهداری اطلاعات زیست‌سنجی منتقل شده .

از نقطه نظر موضوع، انتقال اطلاعات زیست‌سنجی به یک طرف سوم، در اصل همانند ارائه اطلاعات زیست‌سنجی به طور مستقیم به آن طرف سوم است. بر این اساس، رضایت موضوع ضروری است مگر آنکه بر طبق قانون، عکس آن مجاز باشد. انتقالات مرزی به خصوص در سامانه‌های زیست‌سنجی عملیاتی، از جمله کنترل مرزی و گذرنامه‌های الکترونیکی و غیره، متداول است. به همین دلیل، اهمیت زیادی دارد که در مورد

1 Disclosure

حفظ حریم خصوصی اطلاعات زیست‌سنجی منتقل شده که ممکن است به‌وسیله یک طرف سوم پردازش شود، مراقبت و توجه بیشتری صورت پذیرد.

۶-۴-۳ استفاده

استفاده به دسترسی، پردازش، یا تغییر اطلاعات زیست‌سنجی در داخل یک سازمان اشاره دارد. اطلاعات زیست‌سنجی فقط باید با رضایت موضوع استفاده شوند، مگر آنکه قانون عکس آن را مشخص کرده باشد. اگر سازمان بخواهد اطلاعات زیست‌سنجی جمع‌آوری‌شده را برای مقاصدی غیر از آنچه در حال حاضر برای موضوع تعیین شده، استفاده نماید، باید با ارائه شرح کاملی از سایر اهداف استفاده و مدت حفظ اطلاعات زیست‌سنجی، رضایت موضوع را بدست آورد. باید از عملکرد مرموز، یا استفاده گسترده‌تر از اطلاعات زیست‌سنجی، مانند تعیین وضعیت سلامت یا توارث ژنتیکی موضوع اجتناب شود.

۶-۴-۴ ذخیره‌سازی[1]

همانطور که در شکل ۱ نشان داده شده است، معمولا اطلاعات زیست‌سنجی در یک زیرسامانه ذخیره‌سازی داده‌ها ذخیره می‌شوند، که می‌تواند توزیع‌شده باشد. به منظور برآورده شدن الزامات حفظ حریم خصوصی، ممکن است لازم باشد اطلاعات به گونه ای ذخیره شوند که بتوانند به عنوان یک PII حساس شناخته شوند. توصیه می‌شود سازمانها اطلاعات زیست‌سنجی جمع آوری شده را به‌صورت منطقی یا فیزیکی از دیگر PII های فرد جدا نگه‌دارند، تا تأثیر به خطر افتادن اطلاعات ترکیبی بر حفظ حریم خصوصی موضوع، کاهش یابد. برای اطمینان از محرمانگی و یکپارچگی مرجع زیست‌سنجی و همچنین IR مرتبط با آن، انجام اقدامات حفاظتی مناسب، همانطور که در بند ۶ بحث شد، ضروری می‌باشد. برای ردیابی توزیع و سوء استفاده غیر قانونی از نمونه‌های زیست‌سنجی، می‌توان از شِماهای نهان‌نگاری[2] زیست‌سنجی، همانطور که در پیوست ث توصیف شده است، استفاده کرد. باید از ذخیره نمونه‌های زیست‌سنجی بدست آمده که می‌تواند به عنوان یک PII طبقه بندی شود، اجتناب گردد، مگر آنکه به‌طور کامل ضروری باشد.

۶-۴-۵ بایگانی و پشتیبان گیری داده‌ها

بایگانی، فرآیند ذخیره سازی اطلاعات زیست‌سنجی برای نگهداری طولانی مدت یا دائمی است. هنگامی که سازمان، اطلاعات زیست‌سنجی را با رضایت موضوع جمع آوری می‌نماید، ممکن است این رضایت شامل یک تاریخ انقضا برای تعیین دوره ذخیره سازی اطلاعات زیست‌سنجی اخذشده باشد. حفظ اطلاعات زیست‌سنجی بایگانی شده، پس از تاریخ انقضای آن می‌تواند منجر به نقض شرط رضایت شده و باعث ایجاد خطر نقض

1-Storage
2 -Wingatermark

حریم خصوصی گردد. همچنین محدودیت‌های دسترسی به اطلاعات زیست‌سنجی بایگانی شده، باید برای اطلاعات زیست‌سنجی عملیاتی معادل نیز تکرار شود. هرچند پشتیبان گیری از داده‌ها به دلایلی متفاوت با بایگانی انجام می‌شود، اما درصورتیکه داده‌های پشتیبان به اندازه کافی محافظت نشده و پس از انقضا نابود نشود، تهدید مشابهی را برای حفظ حریم خصوصی معرفی می‌کند. خط‌مشی امنیت/حفظ حریم خصوصی سامانه باید به ذخیره‌سازی امن و کنترل دسترسی به بایگانی و داده‌های پشتیبان حاوی اطلاعات زیست‌سنجی و دیگر اطلاعات شخصی، توجه داشته باشد..

۶-۴-۶ نابودسازی

سازمان یا طرف سومی که اطلاعات زیست‌سنجی به آن اعلام شده است، باید اطلاعات زیست‌سنجی موضوع را در زمانهای زیر به‌صورت ایمن نابود نماید (توجه داشته باشید که این فهرست جامع نیست):

- هدف از جمع آوری اطلاعات زیست‌سنجی به تحقق پیوسته و یا مشخص شده است که دیگر مورد نیاز نیست(نقطه ویرگول)

- دوره نگهداری اطلاعات زیست‌سنجی منقضی شده است.

- موضوع، از رضایت خود برای جمع آوری اطلاعات زیست‌سنجی صرفنظر کرده است، و یا مورد استفاده از اطلاعات زیست‌سنجی تغییر کرده است، ولی موضوع اطلاعات زیست‌سنجی موافق با استفاده جدید نیست.

ضروری است که در هنگام نابودسازی اطلاعات زیست‌سنجی ذخیره شده، به خصوص در مورد منابع ذخیره‌سازی توزیع شده، مطمئن شویم که تمام داده‌های مرتبط شناسایی شده و به‌صورت امن نابود شوند. خط‌مشی امنیتی/حفظ حریم خصوصی سامانه، باید اطلاعات زیست‌سنجی و سایر اطلاعات شخصی را که باید در فهرست داده‌ها برای نابودسازی قرار داده شوند، مشخص نماید. این خط‌مشی باید شامل بایگانی و داده‌های پشتیبان باشد (برای جزئیات بیشتر، بندهای قبلی را ببینید). علاوه‌براین، این سیاست باید رویه‌ها و حفاظتهای مناسب برای اطمینان از نابودسازی کامل و امن داده‌ها را توصیف نماید.

۶-۵ مسئولیت‌های صاحب یک سامانه زیست‌سنجی

صاحب سامانه زیست‌سنجی باید مسوول مدیریت صحیح اطلاعات زیست‌سنجی به‌منظور محافظت از اطلاعات و حراست از حقوق موضوع با توجه به اطلاعات زیست‌سنجی موجود در سازمان باشد. برای برآورده کردن این تعهدات، صاحب سامانه زیست‌سنجی باید:

- ابزارهایی برای موضوع مهیا نماید که بتواند اطلاعات زیست‌سنجی خود را در طی چرخه حیاتشان، شامل زمانی که این اطلاعات را در اختیار اشخاص ثالث قرار می‌دهد، کنترل نماید. این به آن معناست که صاحب سامانه زیست‌سنجی باید در هنگام جمع‌آوری اطلاعات زیست‌سنجی، رضایت موضوع را دریافت نماید.
- سازوکاری برای صرفنظر از رضایت فراهم نماید. موضوع می‌تواند در هر زمان که احساس نیاز کند، درخواست صرفنظر از رضایت خود از یک سازمان و یا هر طرف سومی که اطلاعات زیست‌سنجی را دریافت کرده است، بنماید مگر اینکه قوانین، مقررات یا شرایط و ضوابط خدمات، چیزی غیر از آن را تعریف کند. صاحب سامانه زیست‌سنجی باید ابزارهای مناسب برای درخواست چنین تقاضایی و حذف اطلاعات زیست‌سنجی مربوطه از سامانه زیست‌سنجی را برای موضوع فراهم نماید.
- اقدامات امنیتی مناسب برای حراست در برابر حملات برروی محرمانگی، یکپارچگی و دسترس پذیری اطلاعات زیست‌سنجی و خود سامانه زیست‌سنجی مربوطه را ارائه نماید.
- تضمین نماید که اطلاعات مورد استفاده برای تصمیمات شناسایی یا درستی‌سنجی، تا حد امکان کامل، دقیق و به‌روز می‌باشد. در این حالت، واژه اطلاعات به‌طور کلی به PII، و همچنین اطلاعات زیست‌سنجی مربوط به یک موضوع اشاره دارد. مراجع زیست‌سنجی با کیفیت پایین می‌توانند منجر به پذیرش یک مهاجم به‌وسیله سامانه گردند، که در نهایت می‌تواند بر حفظ حریم خصوصی فرد، تاثیرگذار باشد.
- به درخواستهای موضوع برای دسترسی به اطلاعات زیست‌سنجی وی پاسخ دهد. موضوع می‌تواند از صاحب سامانه زیست‌سنجی درخواست کند که به وی اجازه دیدن اطلاعات زیست‌سنجی خودش را بدهد، سؤالاتی درباره جزئیات استفاده از اطلاعات زیست‌سنجی یا انتقال اطلاعات زیست‌سنجی به طرف سوم بپرسد، ودر صورت لزوم برروی اصلاح هر گونه خطا در اطلاعات اصرار نماید.
- هرگونه رخنه‌ای را که باعث به‌خطرافتادن اطلاعات زیست‌سنجی موضوع شود، اطلاع دهد. صاحب سامانه زیست‌سنجی باید هرگونه رخنه شامل سرقت، گم شدن، آسیب، دفع غیرمجاز یا تغییر غیرمجاز اطلاعات زیست‌سنجی موضوع را اطلاع دهد.

۷ . امنیت و مدلهای کاربرد سامانه زیست‌سنجی

۷-۱ مدلهای کاربرد سامانه زیست‌سنجی

همانطور که در جدول ۵ نشان داده شده است، سامانه‌های زیست‌سنجی می‌توانند با توجه به مکانهایی که مراجع زیست‌سنجی و هویت‌های مرجع در آن‌ها ذخیره شده و یا مقایسه شده اند، طبقه بندی شوند. از لحاظ امنیتی، هر مدل با توجه به نحوه مدیریت هویت‌های مرجع و مراجع زیست‌سنجی در زمان انتقال یا ذخیره، دارای مزایا و معایب خاصی است. از لحاظ مفهومی، مدل‌های زیادی وجود دارند، با این حال این استاندارد ملی، هشت نوع مدل که در حال حاضر در کاربردهای واقعی استقرار یافته‌اند را در نظر می‌گیرد.

جدول ۵ – مدل کاربرد یک سامانه زیست‌سنجی

		ذخیره			
		کارساز	مشتری	نشانه	توزیع شده
مقایسه	کارساز	A		B	G
	مشتری	C	D	E	H
	نشانه			F	

مکان‌ها می‌توانند بصورت زیر توصیف شوند.

- یک کارساز، کامپیوتری است که از طریق شبکه، از راه دور به مشتری متصل شده است. یک «کارساز احراز هویت زیست‌سنجی»، یک شکل از یک کارساز می‌باشد.

- یک مشتری، یک کامپیوتر شخصی یا معادل آن است که یک سامانه عامل همه منظوره را اجرا می‌کند و می‌تواند به شکل یک کیوسک۱ باشد. خصوصیات ضروری یک مشتری این است که خدمات پیشین۲ را برای یک سامانه زیست‌سنجی و رابطها با کارساز و/یا نشانه ارائه می‌کند. یک قطعه حسگر زیست‌سنجی می‌تواند به مشتری متصل، یا در آن تعبیه شود. در این استاندارد ملی PDAها و برخی تلفن‌های همراه هوشمند به‌عنوان مشتری در نظر گرفته می‌شوند.

- یک نشانه۳، یک افزاره۴ فیزیکی قابل حمل با قابلیت پشتیبانی از ذخیره‌سازی مرجع زیست‌سنجی است، و در بعضی موارد اجازه مقایسه زیست‌سنجی را نیز می‌دهد. نشانه‌های مورداستفاده برای ذخیره‌سازی زیست‌سنجه‌ها عبارتند از: کارت حافظه USB، گذرنامه‌های الکترونیک، و کارت‌های هوشمند. کارت‌های هوشمند می‌توانند دربرگیرنده یک برنامه مقایسه بر روی کارت۵ برای مقایسه و تصمیم‌گیری زیست‌سنجی باشند..

یادآوری- حسگر زیست‌سنجی که از طریق یک رابط به مشتری متصل شده است، و پیمانه[۶] حسگر تعبیه شده در یک مشتری را می‌توان به‌عنوان مکان‌های دیگری برای ذخیره سازی و مقایسه در نظر گرفت. با این حال، مشتری‌ها اغلب به حسگرهای زیست‌سنجی مجهز می‌شوند. به همین دلیل، این استاندارد ملی آن‌ها را به عنوان بخشی از مشتری در نظر می‌گیرد.

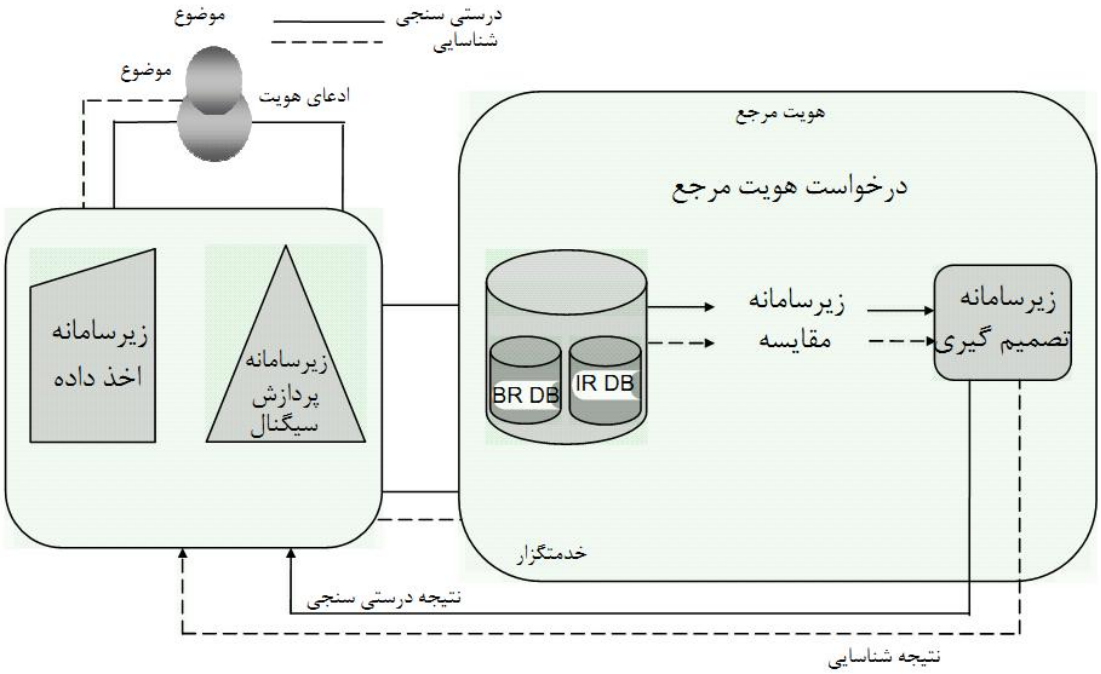
1 -Kiosk
2 -Front end
3 Token
4 -Device
5 Comparison-on-Card application
6 Module

در ادامه، مدل‌های A تا F همبندی‌های[1] مختلفی را برای مکان‌های زیر سامانه‌های مختلف، توصیف می‌نمایند. الزامات امنیتی یکی از عواملی است که تعیین می‌کند بهتر است از مراجع زیست‌سنجی عادی یا تجدیدپذیر استفاده شود. از طرف دیگر، مدل‌های G و H تنها به مراجع زیست‌سنجی تجدیدپذیر (RBRها) اعمال می‌شوند، زیرا این مدل‌ها به منظور افزایش امنیت و حفظ حریم خصوصی سامانه‌های زیست‌سنجی، مفهوم جداسازی داده‌های PI و AD را با توزیع ذخیره‌سازی مابین چندین زیرسامانه ذخیره‌ساز بکار می‌گیرند. به دلیل این جداسازی داده‌ها، مدلهای G و H فقط در مورد فرآیند درستی‌سنجی کاربست‌پذیر هستند.

۷-۲ امنیت در هر مدل کاربرد زیست‌سنجی

۷-۲-۱ مدل A – ذخیره روی کارساز و مقایسه در کارساز

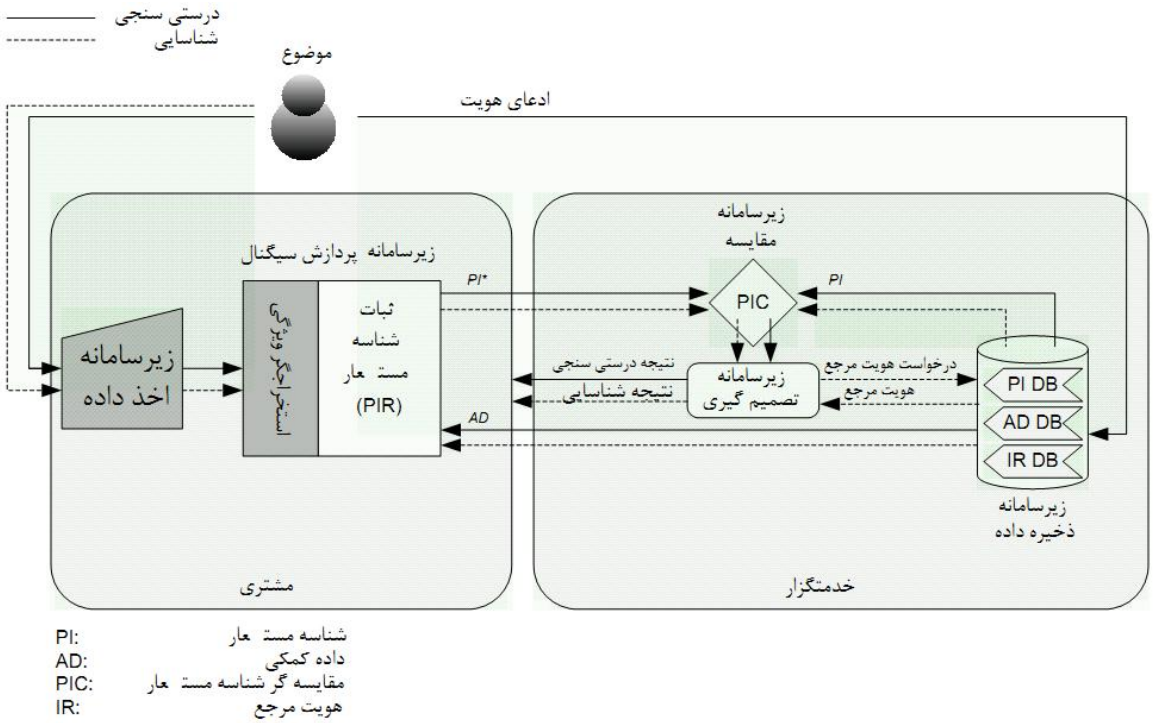
در این مدل، مراجع زیست‌سنجی روی یک کارساز ذخیره می‌شوند و همانطور که در شکل ۶ (برای BRها) و شکل ۷ (برای RBRها) نشان داده شده است، لازم است که داده‌های زیست‌سنجی استخراج شده برای مقایسه به کارساز انتقال پیدا کنند. به‌عنوان بخشی از فرآیند ثبت/ثبت نام، مرجع زیست‌سنجی موضوع به هویت مرجع مربوطه منتسب می‌گردد.



شکل ۶ – مدل A – ذخیره روی کارساز و مقایسه در کارساز با استفاده از BRها

1 -Topology

در این مدل لازم است که کارساز به داده‌های اخذشده از مشتری اعتماد نماید. این مدل می‌تواند برای شناسایی و همچنین درستی‌سنجی مورد استفاده قرار گیرد. از آنجائیکه کارساز PII حساس (یعنی مرجع زیست‌سنجی و هویت مرجع) را به‌کار می‌گیرد، به امنیت دادگان و شبکه قابل اعتماد نیاز داریم. معمولا یک سامانه تجاری شناسایی خودکار اثر انگشت (AFIS[1]) برمبنای این مدل پیاده‌سازی می‌گردد. از نقطه نظر حفظ حریم خصوصی، معمولا این مدل توصیه نمی‌گردد، مگر آنکه مراجع زیست‌سنجی تجدیدپذیر، همانطور که در شکل ۷ با نمونه نشان داده شده است، بکار گرفته شوند، زیرا که در غیراینصورت PII حساس در یک دادگان متمرکز جمع می‌گردد.



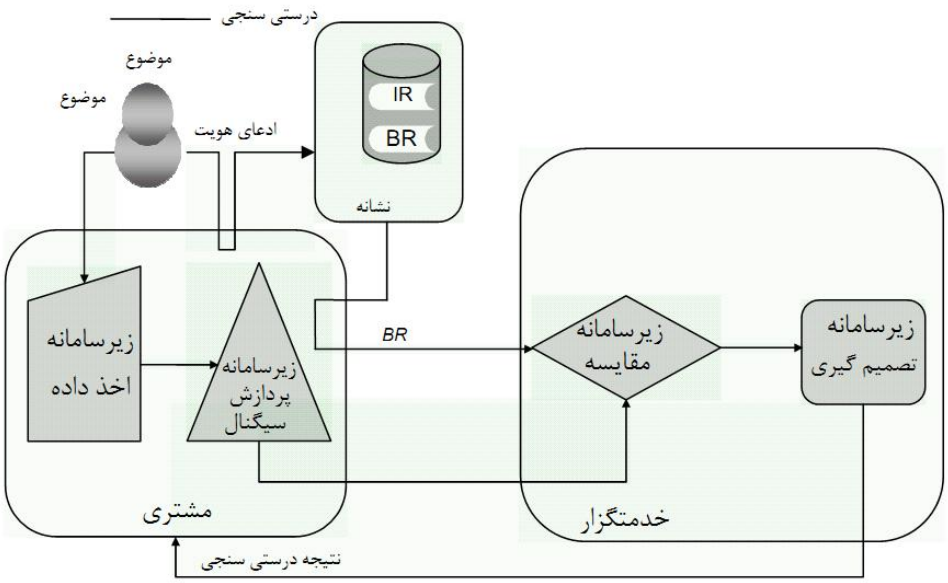
شکل ۷ – مدل A : ذخیره روی کارساز و مقایسه در کارساز از طریق RBRها

۷-۲-۲ مدل B - ذخیره روی نشانه و مقایسه در کارساز

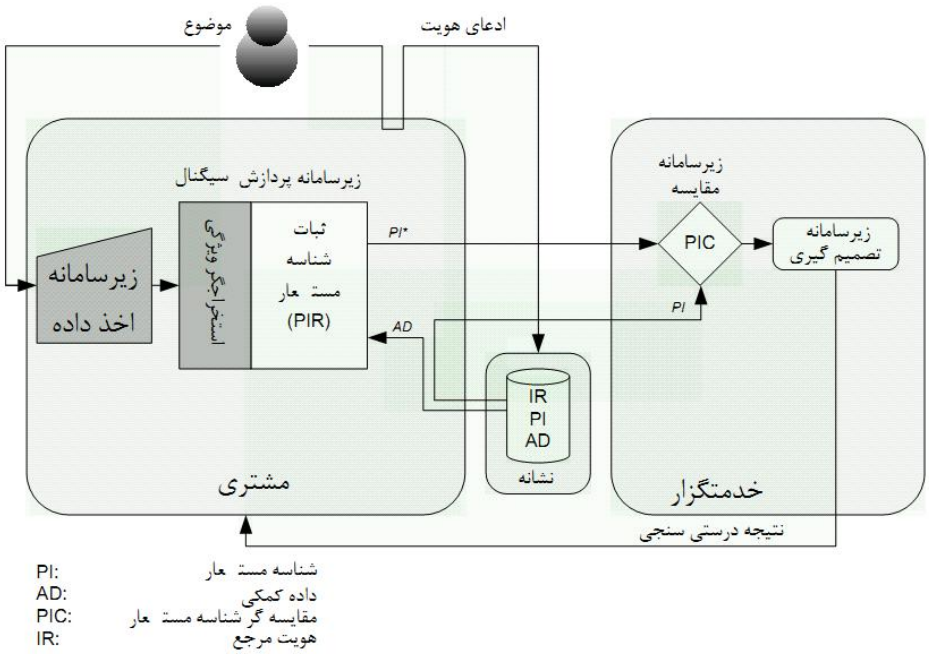
در این مدل، یک نشانه برای ذخیره سازی مراجع زیست‌سنجی استفاده می‌شود و همانطور که در شکل‌های ۸ و ۹ نشان داده شده است، لازم است داده‌های زیست‌سنجی اخذشده برای مقایسه به کارساز منتقل شوند. موضوع زیست‌سنجی در طی فرآیندثبت‌نام، مرجع زیست‌سنجی خود را به هویت مرجع در داخل نشانه نسبت می‌دهد. یک موضوع که می‌خواهد هویت خود را اثبات نماید، باید نشانه را داشته باشد وآن را به

[1] Automated Fingerprint Identification System

مشتری متصل نماید، و همچنین مشخصه(های) زیست‌سنجی خود را ارسال نماید. سپس مشتری هردوی مرجع زیست‌سنجی ذخیره شده، و ویژگی زیست‌سنجی اخذشده را برای مقایسه به کارساز می‌فرستد.
در مورد RBRها، PI که در هنگام ثبت‌نام تولیدشده و سپس بر روی نشانه ذخیره شده است، به همراه*PI که در طی فرآیند درستی‌سنجی بازسازی شده است، به کارساز ارسال می‌گردند درحالیکه AD فقط به مشتری ارائه می‌گردد. این مدل می‌تواند با ذخیره PIها هم برروی نشانه و هم برروی کارساز توسعه یافته و اجازه احراز هویت سه عاملی را بدهد.



شکل ۸- ذخیره روی نشانه و مقایسه در کارساز با استفاده از BRها

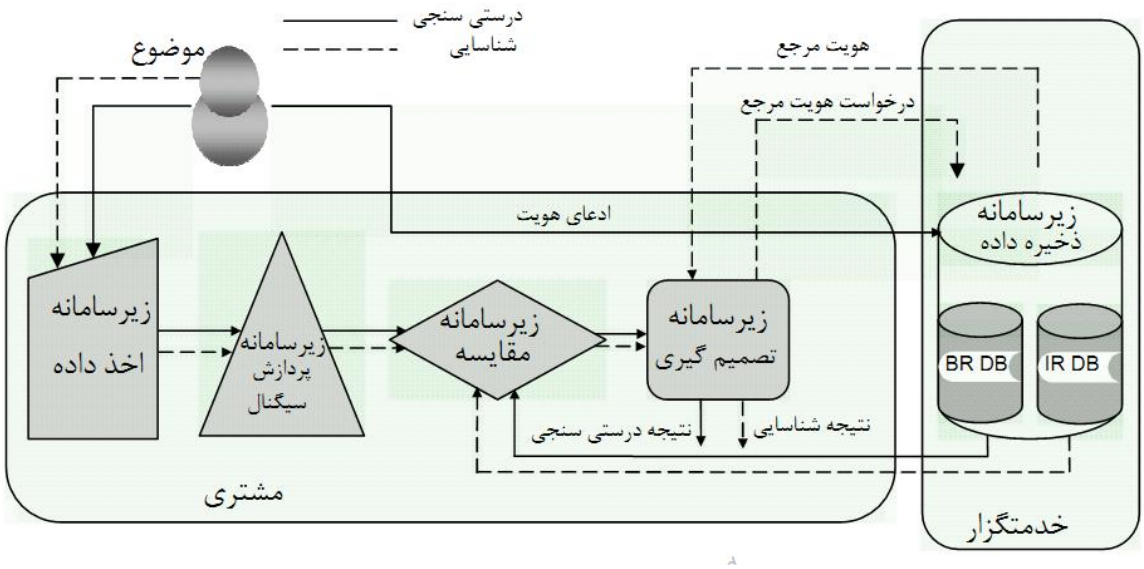


شکل ۹ – مدل B: ذخیره روی نشانه و مقایسه در کارساز با استفاده از RBRها

در این مدل لازم است که کارساز به اطلاعات اخذشده از طرف مشتری اعتماد داشته باشد. معمولا این مدل برای درستی‌سنجی مورد استفاده قرار می‌گیرد، چراکه هیچ مرجع زیست‌سنجی دیگری به جز آنچه به‌وسیله شخص اظهار شده است، برای مقایسه در نشانه وجود ندارد. از آنجا که مرجع زیست‌سنجی در نشانه قابل‌حملی ذخیره می‌شود که می‌تواند به‌صورت امن به‌وسیله فرد بکار رود، این مدل نیاز به امنیت دادگان ندارد. با این حال، برای حفاظت از انتقال مرجع زیست‌سنجی ذخیره شده و داده‌های زیست‌سنجی موردآزمایش اخذشده، این مدل نیاز به امنیت شبکه دارد. اینکار برای آن است که اطمینان حاصل شود کارساز می‌تواند اعتماد کند که داده‌های مرجعی که از مشتری آمده‌اند، ریشه در فرآیند ثبت نام دارند و بلافاصله پیش از درستی‌سنجی در شبکه درج نشده‌اند. توجه شود که هویت مرجع نه منتقل می‌گردد و نه در مشتری و کارساز به مرجع زیست‌سنجی منتسب می‌گردد. بنابراین، این مدل می‌تواند به عنوان یک مدل موافق حریم خصوصی در نظر گرفته شود

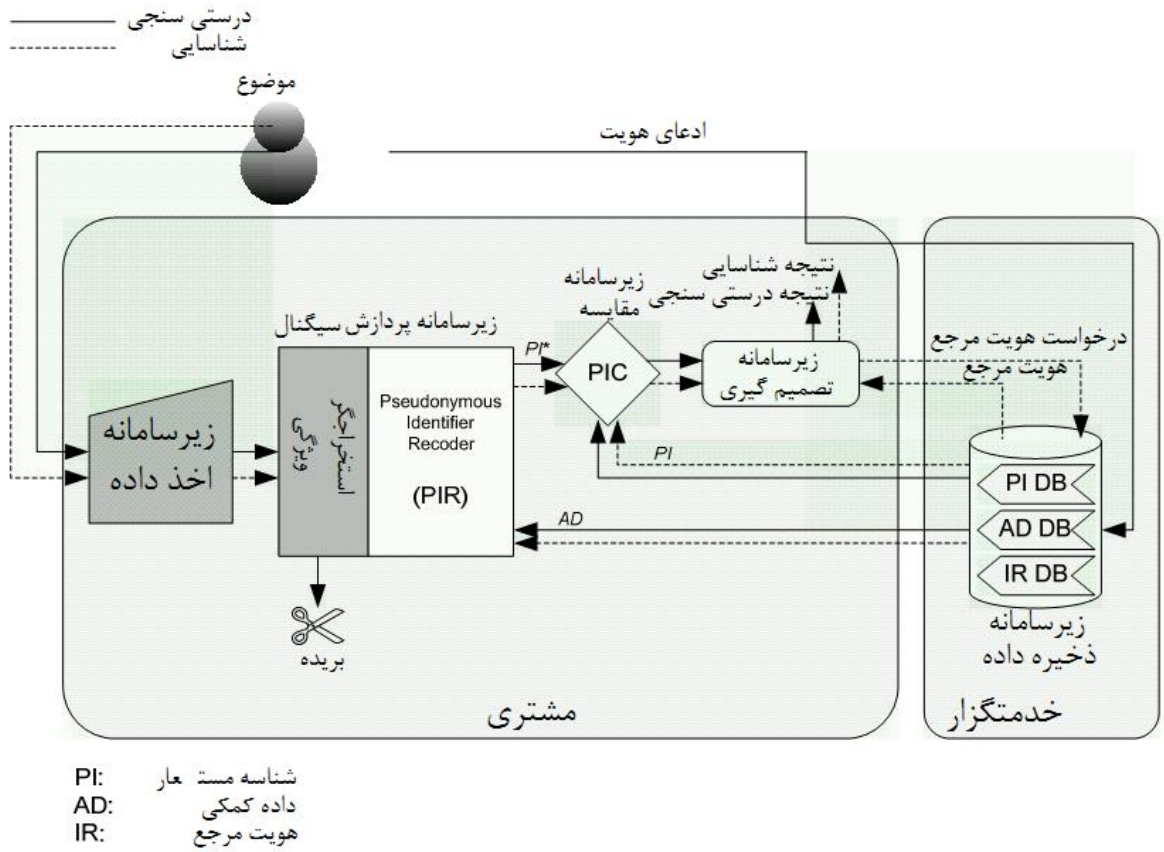
۳-۲-۷ مدل C - ذخیره بر روی کارساز و مقایسه در مشتری

در این مدل، همانطور که در شکل‌های ۱۰ و ۱۱ نشان داده شده است، مراجع زیست‌سنجی بر روی کارساز ذخیره می‌شوند و داده‌های زیست‌سنجی مورد آزمایش در سمت مشتری، برای فرآیند مقایسه، از موضوع استخراج می‌گردند. موضوع زیست‌سنجی، در طی فرآیند ثبت‌نام مرجع زیست‌سنجی خود را به هویت مرجع در کارساز منتسب می‌کند. یک موضوع که می‌خواهد هویت خود را اثبات نماید، نمونه زیست‌سنجی موردآزمایش خود را به مشتری می‌فرستد و سپس مشتری درخواست ارسال مرجع زیست‌سنجی مربوط به موضوع زیست‌سنجی موردادعا را می‌نماید. براساس درخواست، کارساز مرجع زیست‌سنجی ادعاشده را به مشتری می‌فرستد و در نهایت، مشتری مقایسه ای بین نمونه زیست‌سنجی اخذشده و مرجع زیست‌سنجی بارگیری‌شده انجام می‌دهد. برای این مدل، مشتری باید به یک حسگر زیست‌سنجی و همچنین یک الگوریتم مقایسه/تصمیم‌گیری مجهز شود.



شکل ۱۰- مدل C: ذخیره بر روی کارساز و مقایسه روی مشتری با استفاده از BRها

در این مدل لازم است که مشتری به داده‌های دریافت شده از سمت کارساز اعتماد داشته باشد. این مدل می‌تواند برای شناسایی و همچنین درستی‌سنجی استفاده شود. از آنجائیکه PII حساس (یعنی مراجع زیست‌سنجی و هویت‌های مرجع) معمولا در کارساز متمرکز ذخیره می‌شوند، امنیت قابل اعتماد پایگاه داده‌ها و شبکه برای حراست از حریم خصوصی موضوع زیست‌سنجی مورد نیاز است.

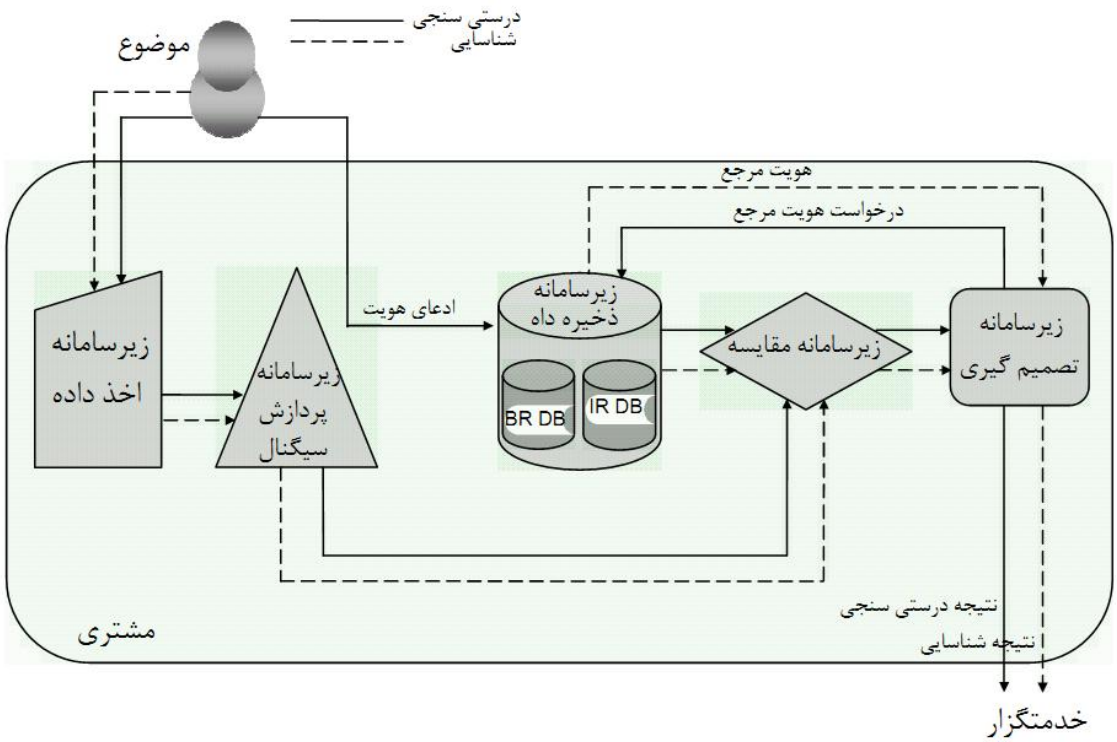


شکل ۱۱- مدل C: ذخیره روی کارساز و مقایسه در مشتری با استفاده از RBRها

۴-۲-۷ مدل D – ذخیره روی مشتری و مقایسه در مشتری

در این مدل، همانگونه که در شکل‌های ۱۲ و۱۳ نشان داده شده است، مراجع زیست‌سنجی روی مشتری ذخیره می‌شوند و یک نمونه زیست‌سنجی موردآزمایش از موضوع زیست‌سنجی، برای فرآیند مقایسه که در مشتری انجام می‌پذیرد، استخراج می‌شود. درطی فرآیند ثبت‌نام، موضوع، مرجع زیست‌سنجی خود را به هویت مرجع بر روی مشتری منتسب می‌نماید. یک موضوع که می‌خواهد هویت خود را اثبات نماید، باید نمونه زیست‌سنجی موردبررسی خود را به مشتری ارسال نماید. برای استقرار این مدل، مشتری باید به یک

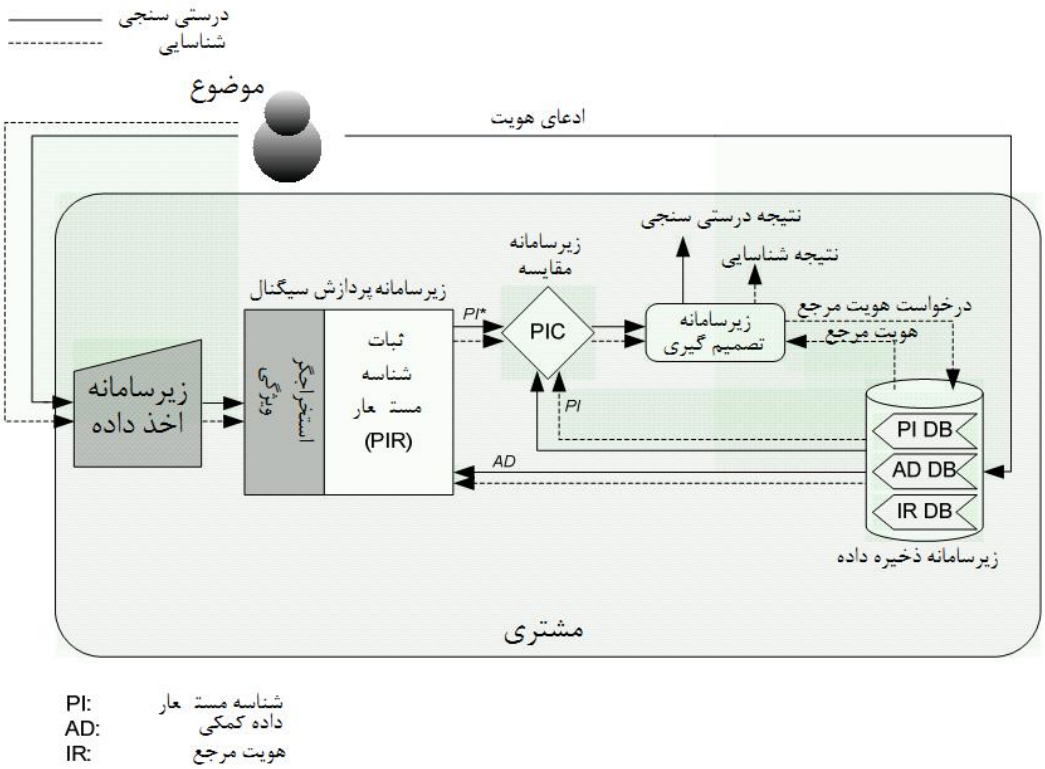
حسگر زیست‌سنجی و یک الگوریتم مقایسه/تصمیم‌گیری مجهز شود. معمولا این مدل برای احراز هویت موضوعاتی که از تجهیزاتی مانند رایانه‌های شخصی رومیزی، لپ‌تاپ [1] و تلفن‌های همراه استفاده می‌کنند، به‌کار گرفته می‌شود. در برخی موارد، مشتری می‌تواند در وضعیت مستقل [2] عمل کند که در آن نیاز به هیچ ارتباطی با کارساز نیست. در سایر موارد، احراز هویت نهایی می‌تواند به‌وسیله کارساز انجام شود، که نتایج درستی‌سنجی ارسالی به‌وسیله مشتری را تایید می‌نماید.



شکل ۱۲ – مدل: D ذخیره بر روی مشتری و مقایسه بر روی مشتری با استفاده از BRها

این مدل می‌تواند برای هردوی شناسایی و همچنین درستی‌سنجی استفاده شود. از آنجایی‌که PII حساس (یعنی مرجع زیست‌سنجی و هویت مرجع) به کارساز منتقل نمی‌شوند، میزان امنیت شبکه می‌تواند کمینه گردد، اگرچه هنوز امنیت پایگاه داده قابل اعتماد برای مشتری موردنیاز است، لذا استفاده از مراجع زیست‌سنجی تجدیدپذیر توصیه می‌گردد. به لحاظ حفظ حریم خصوصی، این مدل مطلوب‌تر از سایر مدل‌هایی است که از یک دادگان متمرکز استفاده می‌کنند.

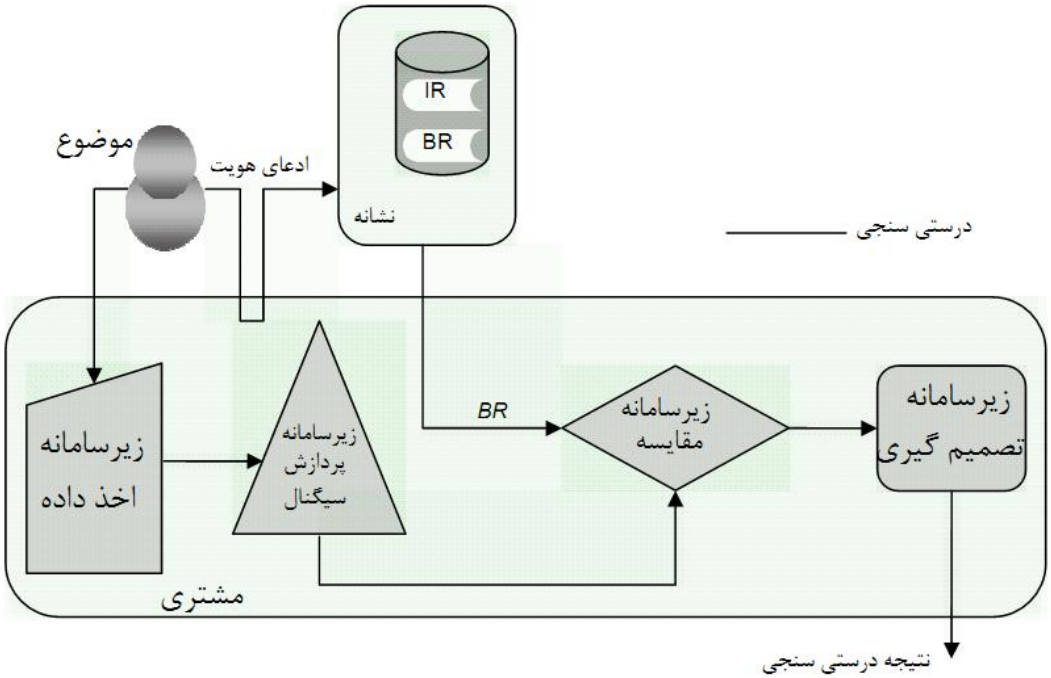
1 -Laptop
2 -Standalone mode



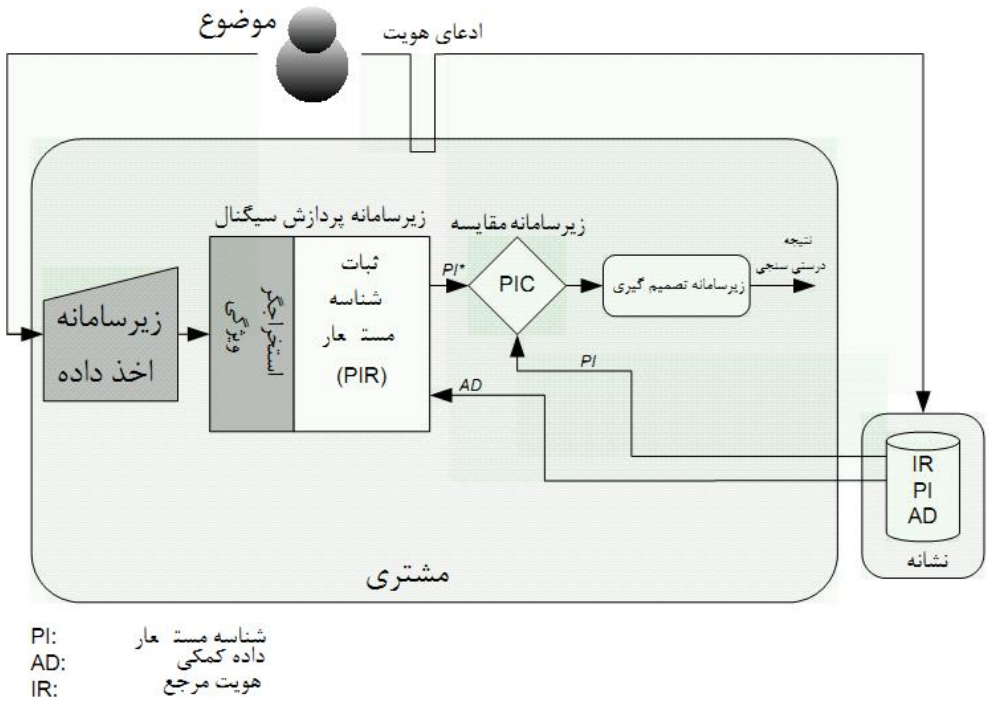
شکل ۱۳ – مدل :D ذخیره بر روی مشتری و مقایسه بر روی مشتری با استفاده از RBRها

۵-۲-۷ مدلE – ذخیره روی نشانه و مقایسه در مشتری

در این مدل، همانطور که در شکل‌های ۱۴ و ۱۵ نشان داده شده است، مراجع زیست‌سنجی روی نشانه ذخیره می‌شوند و یک نمونه زیست‌سنجی موردآزمایش از موضوع زیست‌سنجی، برای فرآیند مقایسه که در مشتری انجام می‌پذیرد، استخراج می‌شود. درطی فرآیند ثبت‌نام، موضوع زیست‌سنجی، مرجع زیست‌سنجی خود را به هویت مرجع بر روی نشانه منتسب می‌نماید. یک موضوع که می‌خواهد هویت خود را اثبات نماید، باید نمونه زیست‌سنجی موردآزمایش خود را به‌همراه نشانه که در داخل آن مرجع زیست‌سنجی قرار دارد، به مشتری ارائه دهد. برای استقرار این مدل، مشتری باید به یک حسگر زیست‌سنجی و یک نرم‌افزار پردازش‌کننده که شامل الگوریتم مقایسه/تصمیم‌گیری می‌باشد، مجهز شود. در اینجا، مشتری می‌تواند از نوع کیوسک باشد، مشابه آنچه که در مکانهای عمومی همانند فرودگاهها و ساختمانهای عمومی برای احراز هویت شخصی پیدا می‌شود. این مدل در کنترل مرزی، با استفاده از گذرنامه الکترونیکی به عنوان نشانه، به‌کار می‌رود.



شکل ۱۴- مدل E: ذخیره روی نشانه و مقایسه بر روی مشتری با استفاده از BRها

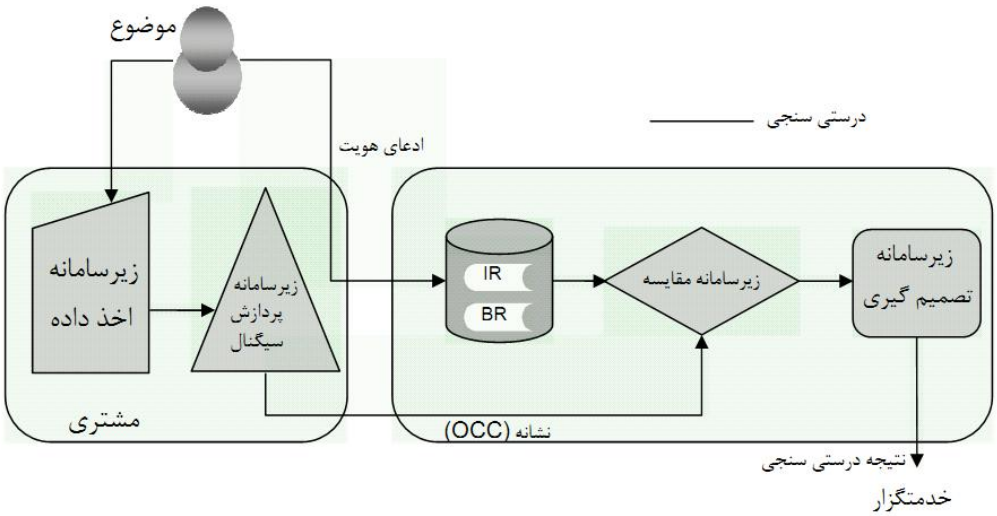


شکل۱۵- مدل E: ذخیره روی نشانه و مقایسه بر روی مشتری با استفاده از RBRها

مراجع زیست‌سنجی و هویت‌های مرجع می‌توانند برروی یک تراشه مدارات مجتمع[1] که در یک نشانه تعبیه شده است، ذخیره شوند. این مدل معمولا برای درستی‌سنجی استفاده می‌شود. از آنجا که PII حساس (یعنی مرجع زیست‌سنجی و هویت مرجع) به کارساز منتقل نمی‌شوند، میزان امنیت شبکه می‌تواند کمینه گردد، هر چند امنیت پایگاه داده قابل اعتماد هنوز هم مورد نیاز است. به لحاظ حفظ حریم خصوصی، این مدل مطلوب تر از سایر مدلهایی است که از ذخیره‌سازی متمرکز برای مرجع زیست‌سنجی و هویت استفاده می‌کنند. توصیه می‌شود فرمان ارسالی به نشانه برای خواندن مرجع زیست‌سنجی، و پاسخ متعاقب آن به‌وسیله نشانه که حاوی داده‌های مرجع زیست‌سنجی است، با استفاده از سازوکارهای انتقال پیام امن در ISO / IEC 7816-4 ایمن شود.

۷-۲-۶ مدل F- ذخیره روی نشانه و مقایسه در نشانه

در این مدل، همانطور که در شکل ۱۶ نشان داده شده است، مراجع زیست‌سنجی بر روی نشانه ذخیره می‌شوند و یک نمونه زیست‌سنجی موردآزمایش از موضوع زیست‌سنجی، برای فرآیند مقایسه که در نشانه انجام می‌پذیرد، استخراج می‌شود. درطی فرآیند ثبت‌نام، موضوع زیست‌سنجی، مرجع زیست‌سنجی خود را به هویت مرجع بر روی نشانه منتسب می‌نماید. یک موضوع که می‌خواهد هویت خود را اثبات نماید، باید نمونه زیست‌سنجی موردآزمایش خود را به‌همراه نشانه به مشتری ارائه دهد (مقایسه برروی کارت [42]). برای استقرار این مدل، نشانه باید به یک الگوریتم مقایسه/تصمیم‌گیری مجهز شود. در اینجا، مشتری می‌تواند یک ماشین خودپرداز (ATM) [2] باشد. این مدل معمولا در تراکنشهای بانکی با استفاده از OCC به‌کار می‌رود.

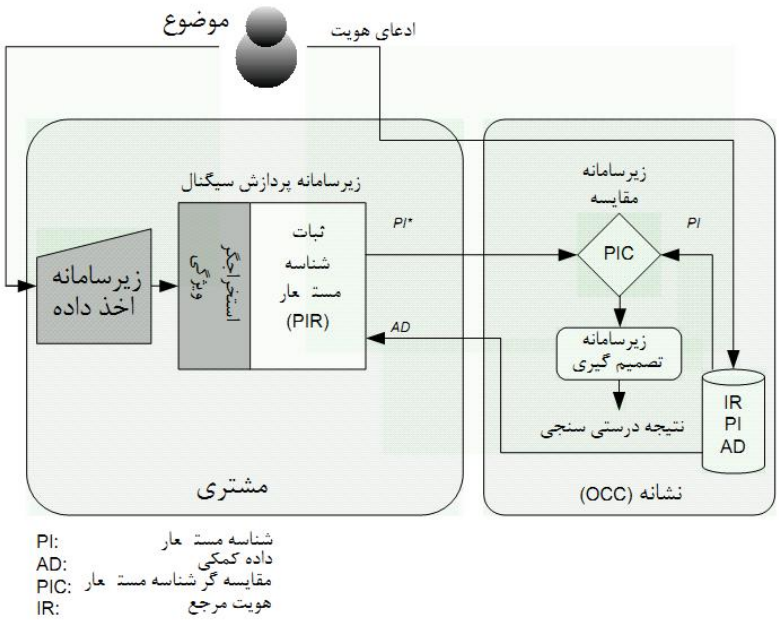


شکل ۱۶ – مدل F: ذخیره روی نشانه و مقایسه در نشانه با استفاده از BRها

1 -IC
2 -Automatic Teller Machine

این نوع از مدل OCC قوی‌ترین سازوکار برای حفاظت از اطلاعات شخصی است. نشانه مقادیر BR و IR را ذخیره می‌کند و فرآیند مقایسه نیز بر روی کارت اجرا می‌شود. نشانه باید قابلیت خود اجرایی[1] داشته باشد. توصیه می‌شود فرمان ارسالی به کارت برای شروع فرآیند مقایسه و پاسخ متعاقب آن به‌وسیله کارت که حاوی نتیجه فرآیند مقایسه است، با استفاده از سازوکار انتقال پیام امن در ISO / IEC 7816-4 ایمن شود. مشتری یک نمونه زیست‌سنجی موردآزمایش و داده IR را بدست آورده و آن‌ها را برای فرآیند مقایسه به نشانه می‌فرستد. نتیجه مقایسه به کارساز فرستاده می‌شود. در اینجا، ممکن است نشانه شامل زیرسامانه پردازش سیگنال باشد. در این حالت، امکان به خطر افتادن اطلاعات زیست‌سنجی موضوع می‌تواند کاهش یابد.

این مدل با ذخیره سازی مرجع زیست‌سنجی و هویت بر روی نشانه، امکان افشای PII یک فرد را محدود می‌سازد. علاوه بر این، برای RBRها (شکل ۱۷ را ببینید)، تنها AD باید به مشتری ارسال شود، در حالی‌که PI در داخل نشانه باقی می‌ماند. بنابراین این مدل می‌تواند به عنوان یک مدل محافظ حریم خصوصی در نظر گرفته شود، چراکه اطلاعات زیست‌سنجی تحت کنترل موضوع هستند. با این حال، مشابه برخی از مدل‌های قبلی، گامهای قابل اعتماد باید در ارتباط مشتری-کارساز تعبیه شوند، به‌طوری‌که کارساز بتواند اطمینان کند که احراز هویت موضوع داده، نتیجه یک مقایسه واقعی است. از طرف دیگر، زیرسامانه‌های اخذ داده‌ها و پردازش سیگنال نیز می‌توانند به‌طور مجتمع در نشانه قرار گیرند. چگونگی پیاده‌سازی مدل F به‌وسیله ISO / IEC 24787 (مقایسه زیست‌سنجی برروی-کارت) استاندارد شده است.



شکل ۱۷ – مدل F: ذخیره روی نشانه و مقایسه در نشانه با استفاده از RBRها

1 -Self-execution

۷-۲-۷ مدل G - ذخیره توزیع شده روی نشانه و کارساز، مقایسه در کارساز

این مدل، از روش تفکیک داده‌ها از طریق ذخیره توزیع شده عناصر داده ای از RBRها، استفاده می‌کند. در طی مرحله ثبت‌نام یک پیاده سازی از این مدل، یک شناساگرشناساگر مستعار ایجاد شده و به همراه شناساگرشناساگر مشترک (CI) در کارساز ذخیره می‌گردد. AD مربوطه، IR و CI روی یک نشانه ذخیره می‌شوند. در طی فرآیند درستی‌سنجی، نشانه AD و CI را برای مشتری منتشر می‌کند (شکل ۱۸ را ببینید). مشتری داده‌های زیست‌سنجی تحت‌آزمایش را اخذ کرده و آن را به یک *PI تبدیل می‌کند. *PI و CI به کارساز منتقل می‌شوند. کارساز، PI و *PI را مقایسه کرده و یک خروجی درستی‌سنجی حاصل می‌شود.

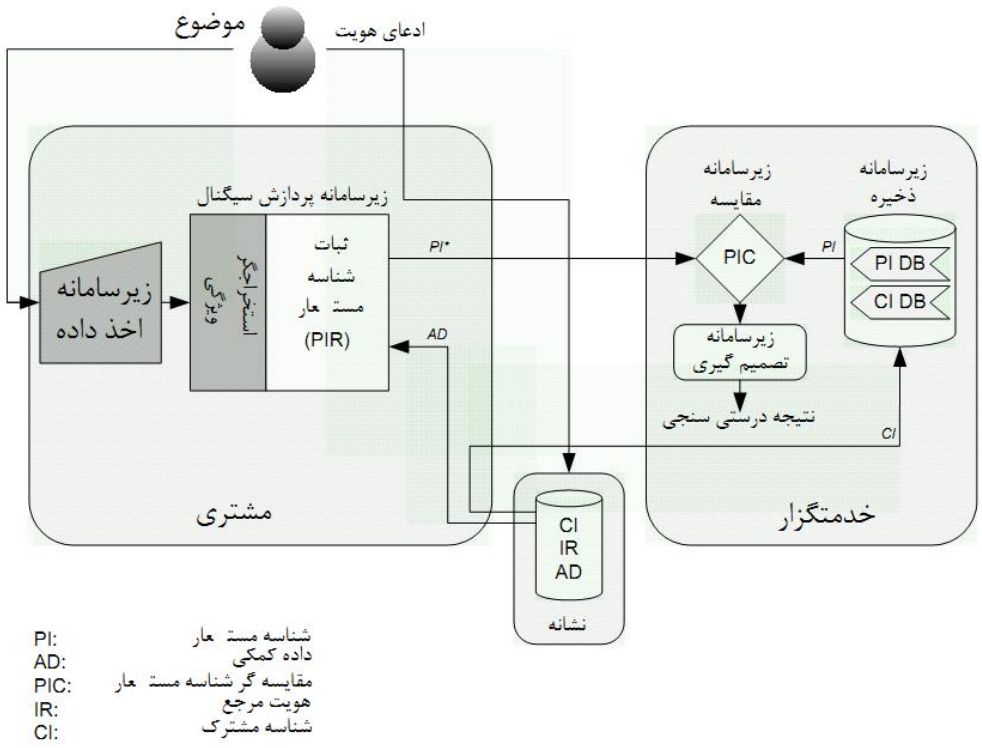
یک مزیت مهم این مدل آن است که مرجع تجدیدپذیر زیست‌سنجی بین نشانه و کارساز توزیع می‌شود. درستی‌سنجی فقط در صورتی امکان‌پذیر است که نشانه و کارساز هر دو حاوی داده‌های صحیح باشند. این خاصیت خطر دستکاری مراجع زیست‌سنجی را کاهش می‌دهد، چراکه نیاز به دستکاری نشانه و همچنین داده‌های کارساز دارد. علاوه بر این، این مدل اجازه ابطال داده‌های مرجع زیست‌سنجی (PIs) را در سمت کارساز، بدون نیاز به دسترسی به یک نشانه می‌دهد. مزیت سوم آن است که موضوع برروی فرآیند درستی‌سنجی کنترل دارد، چراکه به نشانه وی نیاز می‌باشد.

تغییرات/ انطباق‌های زیر می‌توانند در این مدل به کار گرفته شوند:

- IR بجای کارساز، در نشانه ذخیره شود؛
- CI، IR، AD بر روی مشتری و PI، CI بر روی کارساز بدون نیاز به یک نشانه ذخیره گردند؛
- ذخیره سازی PI بر روی نشانه و همچنین بر روی کارساز برای اینکه اجازه احراز هویت سه عاملی در سمت کارساز داده شود. در این پیاده سازی، PIC مقدار PI را از زیرسامانه ذخیره‌سازی کارساز، مقدار PI را از نشانه، و مقدار *PI حاصل از PIR را دریافت می‌نماید.

این مدل به ویژه برای احراز هویت تراکنش برخط[1] (مانند بانکداری الکترونیکی، تراکنش‌های کارت اعتباری برخط و به‌عنوان جایگزین یا توسعه‌ای بر PIN برای دستگاههای خودپرداز) که از یک کارت یا نشانه با قابلیت ذخیره سازی داده‌های کمکی استفاده می‌کند، مناسب می‌باشد. برای کمینه کردن میزان تبادل اطلاعات بین مشتری و کارساز، و جلوگیری از انتقال بخشهایی از داده‌های RBR از کارساز به مشتری، توصیه نمی‌شود که PI بر روی نشانه، و AD درکارساز ذخیره گردند.

1 -Online

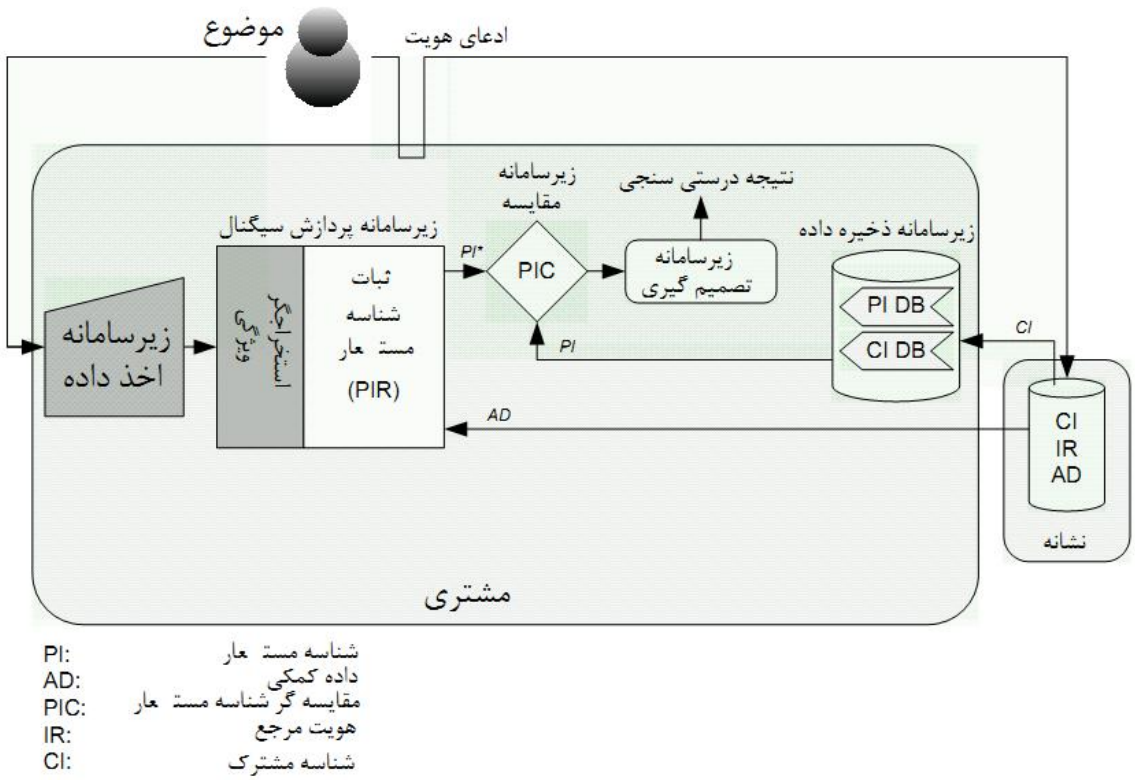


شکل ۱۸- مدل G: ذخیره توزیع شده روی نشانه و کارساز، مقایسه در کارساز

۸-۲-۷ مدل H - ذخیره توزیع شده بر روی نشانه و مشتری، مقایسه در مشتری

در این مدل، مقادیر AD، IR و یک CI بر روی یک نشانه، و مقادیر PI و CI بر روی مشتری ذخیره می‌شوند (شکل ۱۹). در طی درستی‌سنجی، نشانه مقادیر CI و AD را برای مشتری منتشر می‌کند. مشتری مقدار PI مربوط به CI را از زیرسامانه ذخیره سازی خودش بازیابی کرده و AD را به ثبت‌کننده شناساگر مستعار (PIR[1]) انتقال می‌دهد، که بر اساس نمونه تحت‌آزمایش زیست‌سنجی اخذشده، یک شناساگر مستعار نامزد (PI*) تولید می‌کند. PI* حاصل با PI ذخیره شده در مشتری مقایسه شده و نتیجه مقایسه برای تولید یک خروجی درستی‌سنجی به زیرسامانه تصمیم ارسال می‌شود.

1 -Pseudonymous Identifer Recorder



شکل ۱۹ - مدلH : ذخیره توزیع شده بر روی نشانه و مشتری، مقایسه در مشتری

در این مدل، مشتری می‌تواند از نوع کیوسک باشد، مشابه آنچه که در مکانهای عمومی همانند فرودگاهها و ساختمانهای عمومی برای احراز هویت شخصی پیدا می‌شود. همچنین این مدل می‌تواند در تنظیمات کنترل مرزی با استفاده از گذرنامه الکترونیکی (یا یک نشانه دیگر) در یک درخواست مسافر ثبت‌شده، به‌کار رود.
تغییرات زیر می‌توانند برای این مدل به کار گرفته شوند:

- ذخیره IR بر روی مشتری به جای نشانه؛
- ذخیره PI بر روی نشانه و AD در مشتری.

همانطور که در این بند تشریح گردید، معمولا اکثر سامانه‌های زیست‌سنجی از یک کارساز و چند مشتری متصل از راه دورکه مجهز به افزاره‌های اخذ زیست‌سنجی هستند، تشکیل می‌شوند. به‌طورکلی، سطح امنیت کلی فرآیند احراز هویت زیست‌سنجی، وابسته به سطح امنیت فرآیند اجرا شده و همچنین سطح کارآیی کارکردی افزاره‌های اخذ زیست‌سنجی می‌باشد. با به دست آوردن اطلاعات قابل اعتماد مانند سطح کارآیی کارکردی افزاره‌های زیست‌سنجی استفاده شده، و سطح امنیتی سامانه راه دور، و با تعیین اینکه آیا فرآیندها در سامانه به طور امن اجرا شده اند، درستی‌سنج فرآیند احراز هویت می‌تواند تصمیم بهتری راجع به مقدار

قابل اعتماد بودن نتایج درستی‌سنجی مبتنی بر زیست‌سنجی، اتخاذ نماید. برای این کار، زمینه احراز هویت برای زیست‌سنجه‌ها (ACBio[1]) که در ISO/IEC 24761 [۲۰] تعریف شده است، می‌تواند با ارسال اطلاعاتی راجع به افزاره‌های استفاده‌شده و همچنین فرآیند اجرا شده در یک پایگاه[2] راه دور به درستی‌سنج، به‌عنوان یک راه حل برای مشکلات فوق مورد استفاده قرار گیرد.

1 -Authentication Context for Biometrics
2 -Site

پیوست الف

(اطلاعاتی)

انقیاد امن و استفاده از DB_{IR} و DB_{BR} مجزا

الف-۱ عمومی

حتی اگر برای کمینه کردن اثر تجاوز به حریم خصوصی، از دو دادگان برای جدا کردن داده‌های زیست‌سنجی استفاده شود، برای استفاده از آن‌ها باید آن‌ها را با یک شناساگر مشترک CI به یکدیگر متصل کرد. با این حال، هرگز نباید کسی بتواند از روی CI، هرگونه اطلاعات راجع به داده‌ها را استخراج نماید. اگر یک DB مورد حمله قرار گیرد و محتویات آن به خطر بیافتد، متصدیان دو DB باید قادر به کشف آن باشند. به طور مشابه، اگر در طی استفاده از DBها یک متصدی قانونی DB با کلید صحیح، محتوای آن را تغییر دهد، DB دیگر باید قادر به کشف تغییر باشد.

در این پیوست نمونه‌هایی از انقیاد امن یک جفت IR و BR، با فرض دادگان‌های جدا از هم با کنترل مجزا برای IR وBR و کاربردهایشان شرح داده خواهد شد. دادگانهویت‌های مرجع DB_{IR}، و دادگان مراجع زیست‌سنجی DB_{BR} نامیده خواهند شد. فرض می‌کنیم که DB_{IR} از یک کلید محرمانه K_i، و DB_{BR} از یک کلید محرمانه K_b برای محافظت از محتویات دادگانخود استفاده می‌کنند. علاوه بر این، فرض می‌کنیم که دادگان‌ها دو کلید محرمانه را به اشتراک می‌گذارند: K_{ib} برای محاسبه CI و یک مقدار وارسی رمزگذاری[1] و K_e برای امن‌سازی پیام‌های ارتباطی (در صورت نیاز).

الف-۲ انقیاد امن بین DB_{IR} و BR_{DB} مجزا

کانال‌های ارتباطی بین DB_{IR} و DB_{BR} یا امن و یا ناامن هستند، که یک کانال امن به معنای کانالی است که محرمانگی و اعتبار را تامین می‌نماید. در حالت اول (حالت A)، کانال‌های ارتباطی بین دو دادگان امن فرض می‌شوند. در حالت دوم (حالتB)، کانال‌های ارتباطی ناامن فرض می‌شوند، اما دو دادگانیک رمز متقارن و یک کلید محرمانه مشترک K_e را به اشتراک می‌گذارند. انقیاد امن یک مجموعه مشخص از IR و BR در ادامه شرح داده شده است:

حالت A: کانال ارتباطی امن بین DB_{IR} و DB_{BR}

1 -Cryptographic Check Value

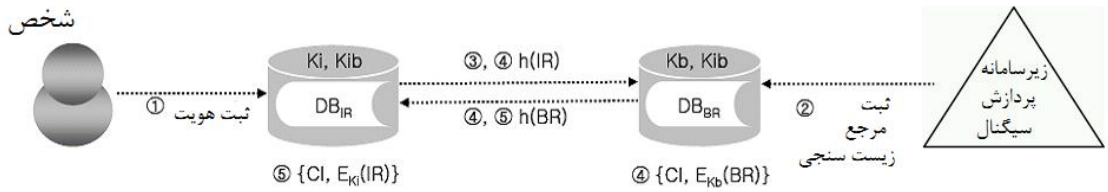
الف) DB_{IR} یک IR معتبر از یک مدعی IR(فرد) و یا یک TTP دریافت کرده، IR را با استفاده از K_i رمزگذاری می‌کند تا $E_{Ki}(IR)$ بدست آید، و همچنین IR را درهم سازی می‌کند تا h(IR) به‌دست آید.

ب) DB_{BR} نیز BR معتبر مربوطه را از زیرسامانه پردازش سیگنال دریافت کرده، BR را با استفاده از K_b رمزگذاری می‌کند تا E_{kb} (BR) به‌دست آید، و سپس BR را درهم‌سازی می‌کند تا h(BR) به‌دست آید.

پ) DB_{IR}، h(IR) را به DB_{BR} می‌فرستد.

ت) DB_{BR}، h(IR) را از DB_{IR} دریافت کرده، مقدار MAC را برای {h(IR), h(BR)} با استفاده از کلید محرمانه مشترک K_{ib} محاسبه می‌کند تا $CI=MAC_{Kib}(h(IR),h(BR))$ به‌دست آید که CI به عنوان یک شناساگر مشترک و همچنین یک مقدار وارسی رمزگذاری استفاده خواهد شد، سپس h(BR) را به DB_{IR} می‌فرستد، و $\{CI, E_{Kb}(BR)\}$ را ذخیره می‌کند.

ث) DB_{IR}، h(BR) را از DB_{BR} دریافت کرده ، مقدار MAC را برای {h(IR), h(BR)} با استفاده از کلید محرمانه مشترک K_{ib} محاسبه می‌کند تا $CI=MAC_{Kib}(h(IR), h(BR)$ به‌دست آید، و سپس $\{CI, E_{Ki}(IR)\}$ را ذخیره می‌کند.



شکل الف۱- انقیاد امن بین DB_{IR} و DB_{BR} مجزا (حالت A)

حالت B: کانال‌های ارتباطی ناامن بین DB_{IR} و DB_{BR}، با کلید محرمانه مشترک K_e

الف) DB_{IR} یک IR معتبر از یک مدعی IR (فرد) و یا از یک TTP دریافت می‌کند، IR را با استفاده از K_i رمزگذاری می‌کند تا $E_{Ki}(IR)$ به‌دست آید، IR را درهم‌سازی می‌کند تا h(IR) به‌دست آید، و سپس {h(IR), $IDDB_{IR}$, $IDDB_{IR}$ N_i} را با استفاده از K_e رمزگذاری می‌کند تا $E_{Ke}(h(IR),$ N_i) به دست آید، که در آن

IDDB یک شناساگر یکتا برای DB است و N_i یک مقدار لحظه‌ای[1] (مهر زمانی یا شماره ترتیب) تولید شده به‌وسیله DB_{IR} است.

ب) DB_{BR}، BR معتبر مربوطه را از زیرسامانه پردازش سیگنال دریافت کرده، BR را با استفاده از K_b رمزگذاری می‌کند تا $E_{Kb}(IR)$ به‌دست آید، و سپس BR را درهم‌سازی می‌کند تا h(BR) به‌دست آید.

پ) DB_{IR} ، $E_{Ke}(h(IR), IDDB_{IR}, N_i)$ را به DB_{BR} میفرستد.

ت) DB_{BR}، $E_{Ke}(h(IR), IDDB_{IR}, N_i)$ را از DB_{IR} دریافت می‌کند، آن را رمزگشایی می‌کند تا {h(IR), $IDDB_{IR}$, N_i}، بازیابی گردد، و سپس $IDDB_{IR}$ و N_i را وارسی می‌کند (اگر وارسی با شکست مواجه شود، با یک پیغام خطا متوقف می‌شود). DB_{BR} مقدار MAC را برای {h(IR), h(BR)} با استفاده از کلید محرمانه مشترک K_{ib} محاسبه می‌کند تا $CI=MAC_{Kib}(h(IR), h(BR))$ به‌دست آید که CI به عنوان یک شناساگر مشترک، و همچنین یک مقدار وارسی استفاده خواهد شد، سپس{CI, h(BR), $IDDB_{BR}$, N_b} را با استفاده از K_e رمزگذاری می‌کند تا$E_{Ke}(CI, h(BR), IDDB_{BR},N_b)$ به‌دست آید، $E_{Ke}(CI, h(BR), IDDB_{BR},N_b)$ را به DB_{IR} ارسال می‌کند، و {CI, $E_{Kb}(BR)$} را ذخیره می‌کند.

ث) DB_{IR}، $E_{Ke}(CI, h(BR), IDDB_{BR},N_b)$ را از DB_{BR} دریافت کرده، $E_{Ke}(CI, h(BR), IDDB_{BR},N_b)$ را رمزگشایی می‌کند تا {CI, h(BR), $IDDB_{BR}$,N_b} به‌دست آید، و سپس $IDDB_{BR}$ و N_b را وارسی می‌کند (اگر وارسی با شکست مواجه شود، با یک پیغام خطا خارج می‌شود). DB_{IR}، MAC را برای {h(IR), h(BR)} با استفاده از کلید محرمانه مشترک K_{ib} محاسبه می‌کند تا $CI=MAC_{Kib}(h(IR),h(BR))$ به‌دست آید، سپس آن را با CI دریافت‌شده مقایسه می‌کند (اگر مقایسه با شکست مواجه شود، با یک پیغام خطا خارج می‌شود)، و {CI, $E_{Ki}(IR)$} را ذخیره می‌کند.

الف-۳ ادعای BR برای درستی‌سنجی

در این زیربند، مثالی از یک ادعای BR از DB_{IR} به DB_{BR} برای درستی‌سنجی توصیف خواهد شد. در اینجا فرض می‌شود که روش پیدا کردن $E_{Ki}(IR)$ صحیح از یک ادعای هویت قانونی داده شده است.

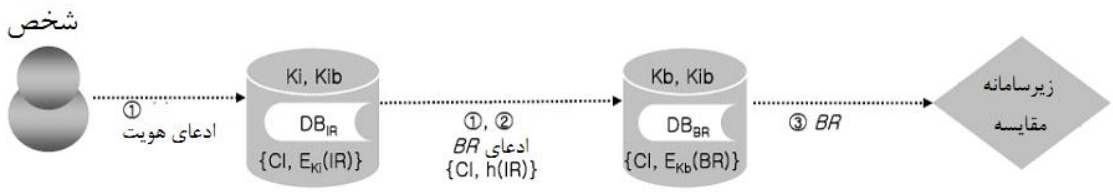
1 -Nonce

حالت A: کانال ارتباطی امن بین DB_{IR} و DB_{BR}

الف) به محض دریافت یک ادعای هویت قانونی از یک مدعی IR(فرد) و یا از یک TTP، DB_{IR} مقدار $E_{Ki}(IR)$ مربوطه را رمزگشایی می‌کند تا IR به‌دست آید، و سپس IR را درهم‌سازی می‌کند تا h(IR) به‌دست آید، و {CI,h(IR)} را به DB_{BR} می‌فرستد.

ب) DB_{BR} مقدار {CI, h(IR)} را از DB_{IR} دریافت کرده، $E_{Kb}(BR)$ را با استفاده از CI پیدا می‌کند، $E_{Kb}(BR)$ را رمزگشایی می‌کند تا BR به‌دست آید، سپس BR را درهم‌سازی می‌کند تا h(BR) به‌دست آید،($MAC_{Kib}(h(IR), h(BR))$ را محاسبه کرده و آن را با CI دریافت شده مقایسه می‌کند.

پ) اگر با یکدیگر مطابق بودند، DB_{BR} مقدار BR را به صورت امن به زیرسامانه مقایسه می‌فرستد. اگر مطابقت با شکست مواجه شود، با یک پیغام خطا خارج می‌شود.



شکل الف۲- ادعای BR برای درستی‌سنجی (حالت A)

حالت B: کانال ارتباطی ناامن بین DB_{IR} و DB_{BR}، با کلید محرمانه اشتراکی K_{ib}

الف) به محض دریافت یک ادعای هویت قانونی از یک مدعی IR(فرد) و یا ازیک TTP، DB_{IR} مقدار $E_{Ki}(IR)$ مربوطه را رمزگشایی می‌کند تا IR به‌دست آید، و IR را درهم‌سازی می‌کند تا h(IR) به‌دست آید، سپس {CI, h(IR), $IDDB_{IR}$, N_i} را رمزگذاری می‌کند تا $E_{Kib}(CI, h(IR), IDDB_{IR}, N_i)$ به دست آید، و $E_{Kib}(CI, h(IR), IDDB_{IR}, N_i)$ را به DB_{BR} می‌فرستد.

ب) DB_{BR}، مقدار $E_{Kib}(CI, h(IR), IDDB_{IR}, N_i)$ را از DB_{IR} دریافت کرده، آن را رمزگشایی می‌کند تا {CI, h(IR), $IDDB_{IR}$, N_i} به‌دست آید، و $IDDB_{IR}$ و N_i را وارسی می‌کند (اگر وارسی با شکست مواجه شود، با یک پیغام خطا خارج می‌شود)، $E_{Kb}(BR)$ را با استفاده از CI پیدا می‌کند، $E_{Kb}(BR)$ را رمزگشایی می‌کند تا BR به‌دست آید، BR را درهم‌سازی می‌کند تا h(BR) به‌دست آید، $MAC_{Kib}(h(IR), h(BR))$ را محاسبه کرده و آن را با CI دریافتی مقایسه می‌کند.

پ) اگر با یکدیگر مطابق بودند، DB_{BR}، BR را به‌صورت امن به زیر سامانه مقایسه می‌فرستد. اگر مطابقت با شکست مواجه شود، ا یک پیغام خطا خارج می‌شود.

الف-۴ ادعای IR برای شناسایی

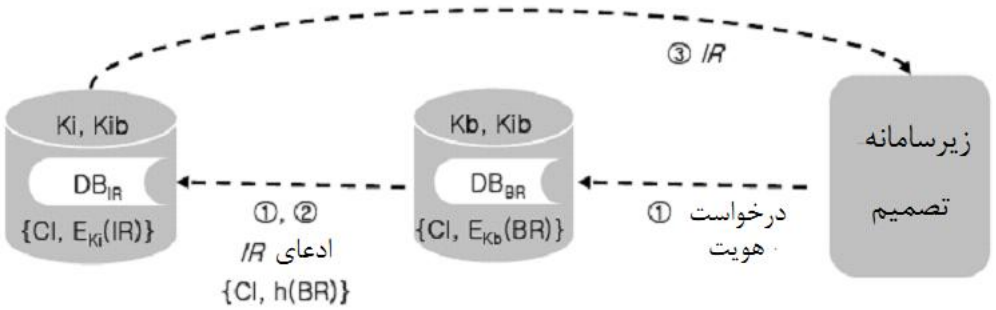
در این زیربند، مثالی از یک ادعای IR از DB_{BR} به DB_{IR} برای درستی‌سنجی توصیف خواهد شد. در اینجا، فرض می‌شود DB_{BR} هم‌اکنون $E_{Kb}(BR)$ را رمزگشایی کرده و BR را به‌دست آورده است، و آن را به زیرسامانه مقایسه ارسال کرده است.

حالت A: کانال ارتباطی امن بین DB_{IR} و DB_{BR}

الف) به‌محض دریافت یک درخواست هویت قانونی از زیرسامانه تصمیم، DB_{BR} مقدار BR را درهم‌سازی می‌کند تا h(BR) به‌دست آید، و {CI, h(BR)} را به DB_{IR} می‌فرستد.

ب) DB_{IR} مقدار {CI, h(BR)} را از DB_{BR} دریافت کرده، $E_{ki}(IR)$ را با استفاده از CI پیدا می‌کند، $E_{ki}(IR)$ را رمزگشایی می‌کند تا IR به‌دست آید، IR را درهم‌سازی می‌کند تا h(IR) به‌دست آید، $MAC_{Kib}(h(IR),$ h(br)) را محاسبه می‌کند، و آن را با CI دریافتی مقایسه می‌کند.

پ) اگر با یکدیگر مطابق بودند، DB_{IR} مقدار IR را به‌صورت امن به زیرسامانه تصمیم می‌فرستد. اگر مطابقت با شکست مواجه شود، با یک پیغام خطا خارج می‌شود.



شکل الف۳- ادعای IR برای شناسایی (حالت A)

حالت B: کانال ارتباطی ناامن بین DB_{IR} و DB_{BR}، با کلید محرمانه مشترک Kib

الف) به‌محض دریافت یک درخواست هویت قانونی از زیرسامانه تصمیم، DB_{BR} مقدار BR را درهم‌سازی می‌کند تا h(BR) به‌دست آید، {CI, h(BR), $IDDB_{BR}$,N_b} را رمزگذاری می‌کند تا E_{Ke}(CI, h(BR), $IDDB_{BR}$,N_b) به‌دست آید، که در آن N_b یک مقدار لحظه‌ای تولید شده به‌وسیله DB_{BR} می‌باشد، و E_{Ke}(CI, h(BR), $IDDB_{BR}$,N_b) را به DB_{IR} می‌فرستد.

ب) DB_{IR} مقدار E_{Ke}(CI, h(BR), $IDDB_{BR}$,N_b) را از DB_{BR} دریافت کرده، آن را رمزگشایی می‌کند تا {CI, h(BR), $IDDB_{BR}$,N_b} بازیابی گردد، و $IDDB_{BR}$ و N_i را وارسی می‌کند (اگر وارسی با شکست مواجه شود، با یک پیغام خطا خارج می‌شود)، E_{ki}(IR) را با استفاده از CI پیدا می‌کند، E_{ki}(IR) را رمزگشایی می‌کند تا IR به‌دست آید، IR را درهم‌سازی می‌کند تا h (IR) به‌دست آید، MAC_{Kib}(h(IR), h(BR)) را محاسبه می‌کند، و آن را با CI دریافتی مقایسه می‌کند.

پ) اگر با یکدیگر مطابق بودند، DB_{IR} مقدار IR را به‌صورت امن به زیرسامانه تصمیم می‌فرستد. اگر مطابقت با شکست مواجه شود، با یک پیغام خطا خارج می‌گردد.

پیوست ب

(اطلاعاتی)

الگوریتم‌های رمزگذاری برای امنیت سامانه‌های زیست‌سنجی

ب-۱ الگوریتم‌های رمزگذاری تامین کننده محرمانگی

برای تامین محرمانگی داده‌ها، الگوریتم‌های رمز نگاری می‌توانند مورد استفاده قرار گیرند. یک الگوریتم رمزگذاری به داده‌ها (که اغلب متن اولیه[۱] یا متن واضح[۲] نامیده می‌شوند) اعمال می‌شود تا داده‌های رمزشده (یا متن رمزی[۳]) به‌دست آید: این فرآیند به‌عنوان رمزگذاری شناخته می‌شود. الگوریتم رمزگذاری به گونه ای طراحی می‌شود که متن رمزی هیچ اطلاعاتی، به‌جز احتمالا طول آن، در مورد متن واضح به دست نمی‌دهد. به هر الگوریتم رمزگذاری، یک الگوریتم رمزگشایی مربوطه منتسب شده است که متن رمزی را به متن واضح اولیه آن تبدیل می‌کند.

رمزها در ارتباط با یک کلید عمل می‌کنند. در یک رمز متقارن، یک کلید یکسان در هر دو الگوریتم رمزگذاری و رمزگشایی استفاده می‌شود. استانداردهای ISO/IEC 18033-3 [۱] و ISO/IEC 18033-4 [۱۵] به دو کلاس مختلف از رمزهای متقارن اختصاص داده شده اند: رمزهای قطعه‌ای[۴] و رمزهای جریانی[۵]. کلید مورد استفاده در یک رمز متقارن به عنوان یک کلید محرمانه[۶] نامیده می‌شود. در یک رمز نامتقارن، برای رمزگذاری و رمزگشایی از کلیدهای متفاوت اما مرتبط استفاده می‌شود. ISO / IEC 18033-2، [۱۳] به رمزهای نامتقارن اختصاص داده شده است. رمزهای نامتقارن از یک کلید رمزگذاری عمومی و یک کلید رمزگشایی خصوصی استفاده می‌کنند. در عمل، از رمزهای کلید متقارن بیشتر از رمزهای نامتقارن برای رمزگذاری داده‌های زیست‌سنجی استفاده می‌شود.

ب-۲ الگوریتم‌های رمزگذاری تامین یکپارچگی

می‌توان از یک الگوریتم کد تایید اصالت پیام (MAC[۷])، یا یک الگوریتم امضای رقمی، برای تامین یکپارچگی داده‌ها استفاده کرد. الگوریتم‌های MAC می‌توانند به عنوان سازوکارهای یکپارچگی داده‌ها، برای تایید عدم

1 -Plaintext
2 -Cleartext
3 -Ciphertext
4 -Block ciphers
5 -Straem ciphers
6 -Secret key
7-Message Authentication Code

تغییر داده‌ها به شیوه ای غیر مجاز استفاده شوند. این الگوریتم‌ها همچنین می‌توانند به‌عنوان سازوکارهای تأیید اصالت پیام مورد استفاده قرار گیرند، برای تضمین اینکه یک پیام از هستاری که کلید محرمانه را دراختیار دارد، نشات گرفته است. دو نوع MAC وجود دارد: سازوکارهایی را که از یک رمز قطعه‌ای استفاده می‌کنند (مطابق با [ISO/IEC 9797-1 ۱۰])، و سازوکارهایی را که از یک تابع درهم سازی اختصاصی استفاده می‌کنند (ISO/IEC 9797-2 [۱۰] را ببینید).

امضاهای دیجیتال می‌توانند بجای امضاهای دست‌نویس برای پیاده سازی خدماتی از قبیل احراز هویت هستار و پیام مورد استفاده قرار گیرند. آن‌ها همچنین می‌توانند برای تامین یکپارچگی و انکارناپذیری پیام مورد استفاده قرار گیرند. این خدمات به پیام‌های رقمی که رشته‌هایی از بیت‌ها هستند (به عنوان مثال، دنباله‌هایی از عناصر داده‌ای و یا اشیاء) اعمال می‌شوند.

بیشتر شِماهای امضای دیجیتال مبتنی بر یک سامانه کلید-عمومی خاص هستند. این سامانه شامل فرآیندی است که جفت کلیدها (یعنی، یک کلید خصوصی و یک کلید عمومی) را تولید می‌کند؛ فرآیندی که از یک کلید خصوصی استفاده می‌کند؛ و فرآیندی که از یک کلید عمومی استفاده می‌کند. دو نوع شِمای امضای دیجیتالی وجود دارد. اگر کل پیام، یا بخشی از پیام بتواند از روی امضا بازیابی شود، این شِما "شِمای امضای دیجیتالی با امکان بازیابی پیام " نامیده می‌شود (ISO/IEC 9796 [۹] را ببینید). هنگامی که تمام پیام باید ذخیره شده و همراه با امضا ارسال شود، شِما " شِمای امضای دیجیتال با پیوست" نامیده می‌شود (ISO/IEC 14888 [۱۲] را ببینید).

ب-۳ الگوریتم‌های رمزگذاری تامین کننده محرمانگی و یکپارچگی

برای تامین هردوی محرمانگی و یکپارچگی، می‌توان از رمزگذاری به‌همراه یک MAC و یا امضا استفاده کرد. با اینکه این عملیات می‌توانند به روشهای متعددی ترکیب شوند، اما همه ترکیبات این سازوکارها تضمین‌های امنیتی یکسانی را ارائه نمی‌دهند. در نتیجه، بهتر است نحوه دقیق ترکیب سازوکارهای یکپارچگی و محرمانگی برای رسیدن به سطح بهینه امنیت، با جزئیات تعریف گردد. علاوه بر این، در برخی موارد می‌توان با تعریف یک روش واحد پردازش داده‌ها، با هدف تامین همزمان محرمانگی و حفاظت از یکپارچگی، بهبود کارایی قابل توجهی را به دست آورد. در ISO/IEC 19772، [۱۶] سازوکارهای رمزگذاری تایید اصالت‌شده تعریف شده اند. این سازوکارها، روشهایی برای پردازش داده‌ها به منظورتامین همزمان حفاظت از یکپارچگی و محرمانگی می‌باشند. آن‌ها معمولا شامل ترکیب مشخصی از محاسبه یک MAC به‌علاوه رمزگذاری داده‌ها، و یا استفاده از یک الگوریتم رمزگذاری برای ارائه همزمان یکپارچگی و محرمانگی هستند.

پیوست پ

(اطلاعاتی)

چارچوبی برای مراجع زیست‌سنجی تجدیدپذیر

پ-۱ مراجع زیست‌سنجی تجدیدپذیر

مراجع زیست‌سنجی تجدیدپذیر (RBRها) شناساگرهای ابطال‌پذیر/ تجدیدپذیری هستند که یک فرد یا موضوع داده را در یک دامنه خاص، با استفاده از یک هویت دودویی محافظت‌شده که از روی یک نمونه زیست‌سنجی اخذشده ساخته (بازسازی) شده است، نشان می‌دهند. یک مرجع زیست‌سنجی تجدیدپذیر اجازه دسترسی به داده‌های اندازه‌گیری زیست‌سنجی اصلی، الگوی زیست‌سنجی یا هویت واقعی صاحبش را نمی‌دهد. علاوه بر این، مرجع زیست‌سنجی تجدیدپذیر در خارج از دامنه خدمت معنایی ندارد. مراجع تجدیدپذیر زیست‌سنجی ۴ مرحله متمایز را دنبال می‌کنند:

الف) ایجاد RBRهای جدید از داده‌های زیست‌سنجی در طی مرحله ثبت نام؛
ب) استفاده عملیاتی از RBR به عنوان یک مرجع برای سنجش درستی یک هویت ادعا شده؛
پ) انقضای اعتبار RBR؛ و
ت) تجدید و یا فسخ یک RBR در صورت انقضای اعتبار آن و یا به خطر افتادن RBR

پ-۲ ایجاد

زیر سامانه پردازش سیگنال برای فرآیند ایجاد RBR در شکل پ.۱ نشان داده شده است. یک پیکان در این شکل نشان‌دهنده یک جریان اطلاعات است. به‌طورکلی، پیکان نشان‌دهنده یک پروتکل بین دو مرحله[1] است که به‌وسیله مبدا یا مقصد پیکان برقرارشده است. یک مرحله استخراج ویژگی،داده‌های ویژگی زیست‌سنجی را از نمونه زیست‌سنجی اخذشده تولید می‌کند. ترجیحا ویژگیها مطابق با استانداردهای موجود برای داده‌های مرجع زیست‌سنجی، به شکلی که در ISO/IEC 19794-x توصیف شده است، تولید می‌شوند. در ادامه، یک کدبندی‌کننده شناساگر مستعار (PIE)، یک مرجع زیست‌سنجی تجدیدپذیر متشکل از یک شناساگر مستعار و داده‌های کمکی (AD) ایجاد می‌کند. پس از تولید RBR، می‌توان نمونه زیست‌سنجی

1 -Protocol

اخذشده و خصوصیات استخراج شده را دور انداخت. داده‌های کمکی می‌توانند یکی از اهداف زیر را برآورده سازند:

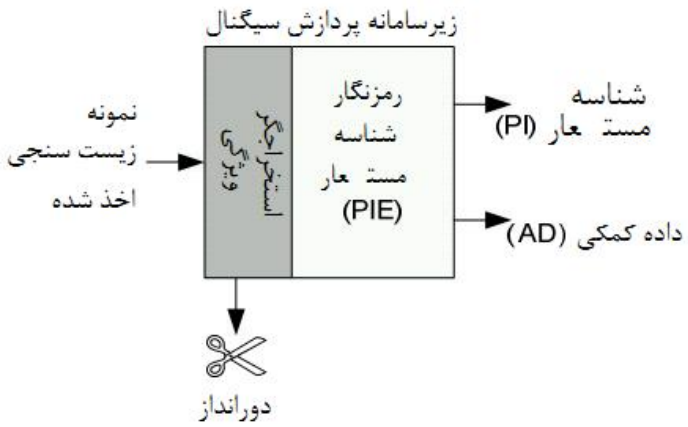
- اجازه ایجاد مجدد یک شناساگر مستعار منتسب به نمونه زیست‌سنجی اخذشده را برای مقایسه با شناساگر مستعار مرجع می‌دهند؛

- اجازه تولید چندین شناساگر مستعار مستقل از یک فرد یکسان را، در درون یک برنامه کاربردی، برای تامین منابع تجدید پذیر می‌دهند؛

- اجازه تولید شناساگرهای مستعار مستقل را، در بین برنامه‌های کاربردی، برای جلوگیری از مقایسه-متقابل و پیوند پایگاه داده می‌دهند؛

- به منظور افزایش امنیت و حفظ حریم خصوصی، ابزاری برای جداسازی داده‌های مرجع زیست‌سنجی (PI و AD) فراهم می‌کنند و

- اجازه استفاده از پارامترهای مقایسه فردی[1] برای بهینه سازی کارآیی درستی‌سنجی را می‌دهند



شکل پ۱- زیر سامانه پردازش سیگنال برای تولید مراجع زیست‌سنجی تجدید پذیر

AD می‌تواند از روش‌های مختلف تهیه مراجع زیست‌سنجی تجدید پذیر، بدست آید (برای یک مرور کلی، پیوست ت را ببینید). PI و AD هر دو ذخیره می‌شوند (یا هر دو با هم به عنوان یک ورودی پایگاه‌داده

1 -Individualized

ترکیبی و یا بر روی رسانه‌ها/پایگاه‌داده‌های ذخیره‌سازی جداگانه)، ولی تمام داده‌های زیست‌سنجی اخذشده دیگر به روشی امن نابود می‌شوند. ترکیبی ازPI و AD، مرجع زیست‌سنجی تجدیدپذیر (RBR) را تشکیل می‌دهد.

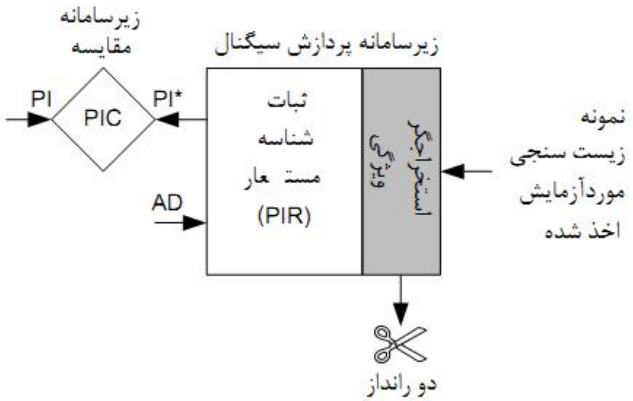
پ-۳ مقایسه

در یک سناریوی مقایسه از راه دور، زیرسامانه‌های اخذ داده‌ها و پردازش سیگنال از یک سو، و زیرسامانه مقایسه از سوی دیگر، از نظر فیزیکی از یکدیگر جدا هستند (شکل پ.۲ را ببینید). درستی‌سنجی، نیازمند مراحل زیر است:

- یک مرحله استخراج ویژگی، نمونه داده‌های زیست‌سنجی موردآزمایش را پردازش می‌کند؛
- یک ثبت‌کننده شناساگر مستعار (PIR) ، بر اساس داده‌های کمکی ارائه‌شده و ویژگیهای استخراج شده، یک شناساگر مستعار جدید (*PI) تولید می‌کند؛

- یک زیر سامانه مقایسه با استفاده از یک مقایسه‌گر شناساگر مستعار (PIC[1])، PI و *PI را مقایسه کرده و یک امتیاز مقایسه تولید می‌کند؛

- یک زیر سامانه تصمیم (در شکل پ.۲ نشان داده نشده است) بر اساس امتیاز مقایسه، یک خروجی درستی‌سنجی ارائه می‌کند.



شکل پ۲- زیرسامانه پردازش سیگنال و زیرسامانه مقایسه

پ-۴ انقضا

1 -Pseudonymous Identifier Comparator

مراجع زیست‌سنجی تجدیدپذیر به چندین دلیل منقضی می‌گردند. به عنوان مثال، ممکن است یک RBR تنها برای یک دوره محدود صادر شده باشد، و یا ممکن است به دلیل اینکه به خطر افتاده است، نیاز به تجدید داشته باشد. علاوه بر این، ممکن است اثرات پیری بر مشخصه‌های زیست‌سنجی تاثیر بگذارد، مانند چهره انسان که نیازمند تجدید مرجع زیست‌سنجی است. وارسی‌های اعتبار و انقضاء می‌توانند از طریق فهرست‌های ابطال، کنترل شوند.

پ-۵ ابطال

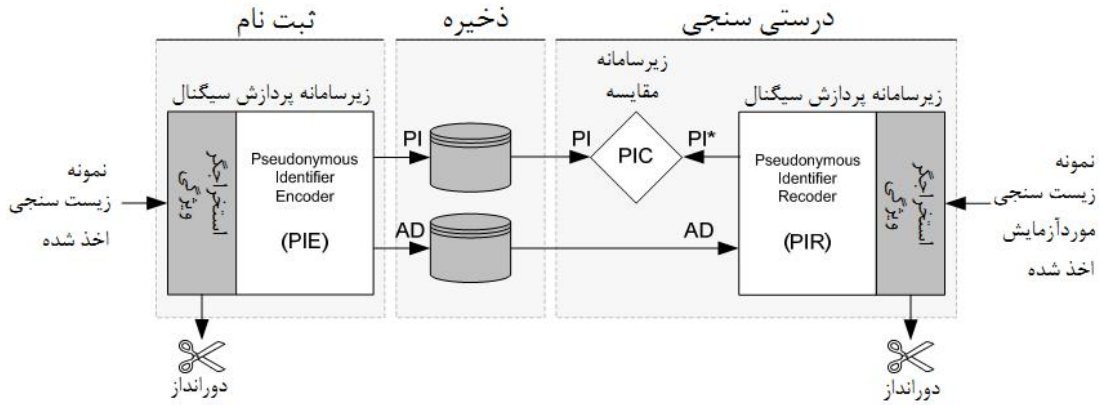
بسته به پیاده سازی یک سامانه درستی‌سنجی، RBR ها می‌توانند به‌صورت زیر باطل شوند:

- حذف RBR از یک پایگاه داده، و/یا
- حذف مجوز استفاده از یک RBR.

پس از ابطال، ثبت نام مجدد می‌تواند منجر به ایجاد یک مرجع زیست‌سنجی تجدیدشده شود. بسته به روش پیاده‌سازی استفاده‌شده، ممکن است این کار نیازمند ضبط نمونه‌های زیست‌سنجی اصلی جدید باشد. در سایر پیاده سازی‌ها، ثبت نام مجدد بر اساس داده‌های زیست‌سنجی خام، و یا RBRهای یدکی ذخیره‌شده در یک پایگاه داده به‌طور کامل امن که هم به صورت منطقی و هم به‌صورت فیزیکی از پایگاه داده عملیاتی RBR جدا شده است، انجام می‌گردد تا اجازه ثبت نام مجدد، بدون حضور فیزیکی موضوع داده را بدهد.

پ-۶ مرور کلی بر معماری

فرآیندهای ثبت نام، ذخیره‌سازی و درستی‌سنجی در شکل پ.۳ ارائه شده اند. زیرسامانه تصمیم‌گیری که به زیرسامانه مقایسه متصل می‌شود، در شکل پ.۳ نمایش داده نشده است.



شکل پ ۳ -معماری مراجع زیست‌سنجی تجدید پذیر

پیوست ت

(اطلاعاتی)

نمونه‌های فناوری برای مراجع زیست‌سنجی تجدیدپذیر

ت-۱ مرور کلی

روش‌های مختلفی برای استخراج مراجع زیست‌سنجی تجدیدپذیر منتشر شده است (می‌توانید برای کسب اطلاعات پیش زمینه‌ای بیشتر، [۳۴] [۳۳] را ببینید.) جدول ت۱، فهرستی از مثالها شامل مراجع و نگاشت بین عناصر داده‌ای مختلف روش و عناصر داده‌ای مشخص شده در این استاندارد ملی را ارائه می‌کند.

جدول ت۱ – مرور کلی روش‌های تولید مراجع زیست‌سنجی تجدیدپذیر

(طبق استاندارد ۵ زیر نویس ها ی این جدول باید به زیر نویس جدول تبدیل شوند)

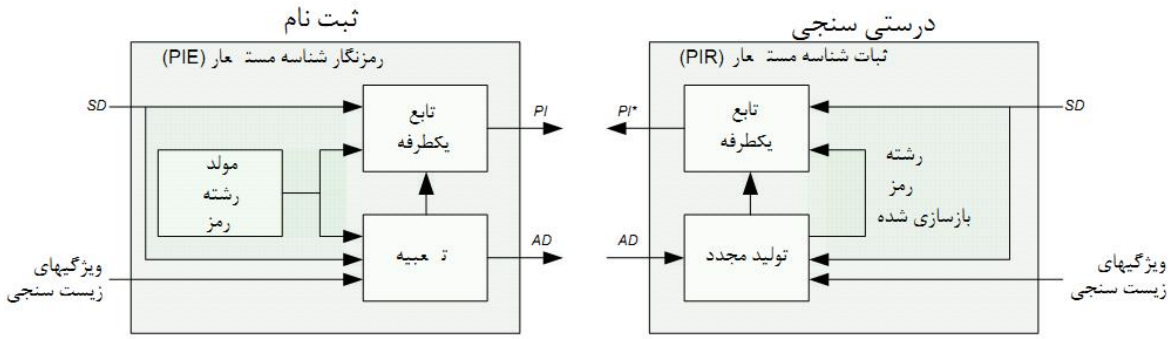
روش	مرجع	شناساگر مستعار (PI)	داده کمکی (AD)
سامانه‌های داده‌های کمک‌کننده[1]	[22]	درهم‌سازی رشته محرمانه	داده‌های کمک‌کننده
التزام فازی	[23]	درهم‌سازی رشته محرمانه	انحراف[2]
رمزگذاری زیست‌سنجی	[24]	کلید رمزگذاری	اتصال کلید و صافی[3]
صندوق فازی[4]	[25]	درهم‌سازی رشته محرمانه	مجموعه نقطه P
کارکردهای حفاظتی	[26]	درهم‌سازی رشته محرمانه	چالش احراز هویت W
استخراج‌کننده‌های فازی[5]	[27]	درهم‌سازی رشته محرمانه	رشته عمومی P
PIR توسعه‌یافته	[28]	الگوی رمزشده	موجود نیست
مدوله‌سازی اندیس کوآنتش[1] شش‌ضلعی دوبعدی[6]	[29]	درهم‌سازی رشته محرمانه	خطاهای کوآنتش
زیست‌سنجی‌های لغوپذیر[7]	[31]	الگوی تبدیل‌یافته	پارامترهای تبدیل
درهم‌سازی قوی[8] زیست‌سنجی	[36]	درهم‌سازی یک رشته دودویی	تبدیل یک‌طرفه

1 Helper Data
2 Offset
3 Filter
4 Fuzzy vault
5 Fuzzy extractor
6 2D hexagonal quantization index modulation
7 Cancellable
8 Robust

		محکم	
درهم‌سازی زیستی۱	[37]	یک رشته دودویی محکم	ماتریس تصویر تصادفی
کلید رمزگذاری کوتاه‌مدت۲	[38]	کلیدهای رمزگذاری	پارامترهای سامانه
نشانه‌های زیستی۳	[39]	جزئیات۴ رمزشده	کلیدهای رمزگذاری
طرح۵ امن	[40]	باقیمانده کوآنتش	کوآنتش‌کننده
درهم‌سازی جزئیات محکم	[41]	رشته دودویی محکم برای هر جزء	جدول متنوع‌سازی تصادفی

1-Quantize

یک روش به‌طور کامل متداول در شکل ت.۱ نشان داده شده است. در طی ثبت نام، کدبندی‌کننده شناساگر مستعار، ویژگیهای زیست‌سنجی را به عنوان ورودی دریافت می‌کند. یک رشته محرمانه به‌وسیله یک مولد رشته محرمانه تولید می‌شود. در ادامه، یک تابع "تعبیه"[۶]، داده‌های کمکی را ("طرح عمومی"[۷] نیز نامیده می‌شوند) با ترکیب ویژگیهای زیست‌سنجی و رشته محرمانه،تولید می‌کند. در بسیاری از پیاده سازی‌های عملی، تابع "تعبیه" حاوی شکلی از کوانتش[۸] (یعنی تبدیل داده‌های ویژگی پیوسته به رشته‌های دودویی) خواهد بود. شناساگر مستعار با استفاده از یک تابع یک طرفه رمزگذاری و رشته محرمانه به‌عنوان ورودیها، و داده‌های کمکی به‌صورت اختیاری، ایجاد می‌شود.



شکل ت۱- پیاده سازی سطح بالا برای تولید مراجع زیست‌سنجی تجدیدپذیر

1 Biohashing
2 Short-lived cryptokey
3 Bio-tokens
4 Minutiae
5 Sketch
6 -Embed
7 -Public sketch
8 -Quantization

در حین درستی‌سنجی، ثبت‌کننده شناساگر مستعار، داده‌های کمکی و ویژگیهای زیست‌سنجی را به عنوان ورودی دریافت می‌کند. یک تابع "بازتولید[1]"، رشته مخفی را بر اساس ویژگیهای زیست‌سنجی و داده‌های کمکی، بازتولید می‌کند. پس از آن، یک شناساگر مستعار (PI*) با استفاده از یک تابع یک طرفه با رشته محرمانه بازسازی شده، تولید می‌شود.
پیاده‌سازی‌های جایگزین می‌توانند از یک ورودی اضافی تولیدشده به‌وسیله کاربر یا سامانه (داده‌های مکمل یا SD[2]) نیز برای تصادفی کردن ویژگیهای زیست‌سنجی، به عنوان بخشی از مرحله تعبیه و یا به‌عنوان ورودی اضافی به تابع یک طرفه استفاده کنند. به‌عنوان مثال، این ورودی می‌تواند شامل یک کلمه‌عبور، کلید و یا PIN محرمانه باشد([۳۲] را ببینید). از طرف دیگر، اگررشته تصادفی‌سازی، عمومی و وابسته به موضوع فرض شود، این رشته می‌تواند بخشی ازAD باشد.

توابع تعبیه و یک طرفه باید الزامات مختلفی را برای حراست از حریم خصوصی برآورده سازند. این الزامات عبارتند از:

- آنتروپی[3] کافی در رشته‌های محرمانه ایجاد شده. این الزام برای داشتن تعداد کافی از متنوع‌سازی‌های RBRها برای یک شخص واحد، موردنیاز است.

- بازگشت‌ناپذیری تابع تولید کدبندی‌کننده شناساگر مستعار برای جلوگیری از بازسازی زیست‌سنجه یا رشته محرمانه از روی PI.

- پیوندناپذیری RBRهایی که با استفاده از ویژگیهای زیست‌سنجی یکسان، برای برنامه‌های کاربردی مختلف تولید شده‌اند، به منظور جلوگیری از تطبیق بین پایگاه داده‌ها[4].

1 -Reproduce
2 -Supplementary data
3 -Entropy
4 -Cross-matching of databases

پیوست ث

(اطلاعاتی)

نهان نگاری[1] زیست‌سنجی

ث-۱ نهان نگاری زیست‌سنجی

نهان نگاری زیست‌سنجی یک روش حفاظت از نمونه زیست‌سنجی است که از اطلاعات مرتبط راجع به سازمان، دوره اعتبار و شناساگرهای یکتای نمونه زیست‌سنجی به عنوان یک نهان‌نگار استفاده می‌کند تا از توزیع و سوء استفاده غیرقانونی از نمونه زیست‌سنجی جلوگیری کند. نهان نگاری زیست‌سنجی همچنین می‌تواند ویژگیهای انکارناپذیری و ردیابی را برای جلوگیری از توزیع غیرقانونی نمونه‌های زیست‌سنجی، تامین کند.

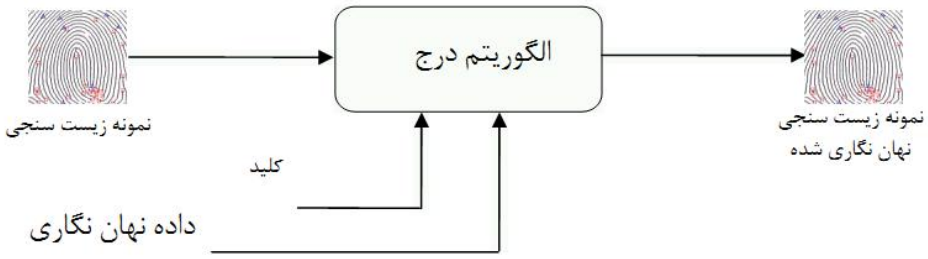
نهان نگاری زیست‌سنجی شامل دو فرآیند اصلی است:

- ایجاد و تعبیه یک نهان‌نگار زیست‌سنجی
- استخراج نهان نگار تعبیه شده از نمونه زیست‌سنجی نهان نگاری شده

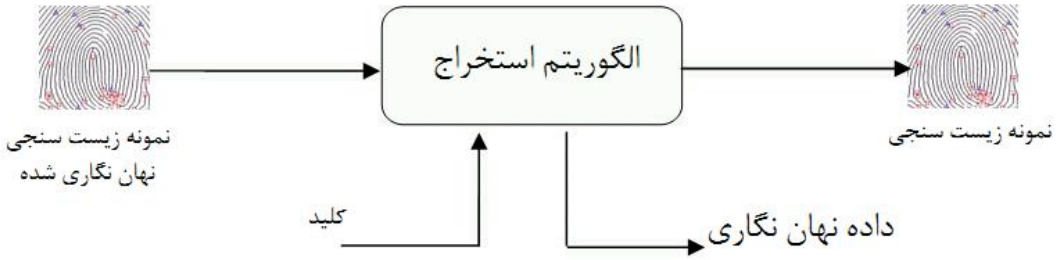
ث-۲ درج و استخراج یک نهان نگار زیست‌سنجی

داده‌های نهان نگار تعبیه شده که حاوی اطلاعات مرتبط درباره نمونه زیست‌سنجی می‌باشند، به نهان نگارهای دو بعدی تبدیل می‌شوند. نهان‌نگار به‌وسیله الگوریتم درج، بدون تغییر شکل[2] نمونه زیست‌سنجی در نواحی مناسب تعبیه می‌شود، و سرانجام نمونه زیست‌سنجی نهان‌نگاری شده به دست می‌آید. فرآیند استخراج، همانطور که در شکل ث.۱ نشان داده شده است، می‌تواند به عنوان فرآیند معکوس فرآیند تعبیه توصیف شود.

1 -Watermarking
2 -Distort



(الف) فرآیند تعبیه برای نهان نگاری زیست‌سنجی



(ب) فرآیند استخراج برای نهان نگاری زیست‌سنجی

شکل ث۱- فرآیندهای نهان نگاری زیست‌سنجی

ث-۳ نمونه‌های کاربرد

- حفاظت نمونه زیست‌سنجی از استفاده غیر مجاز

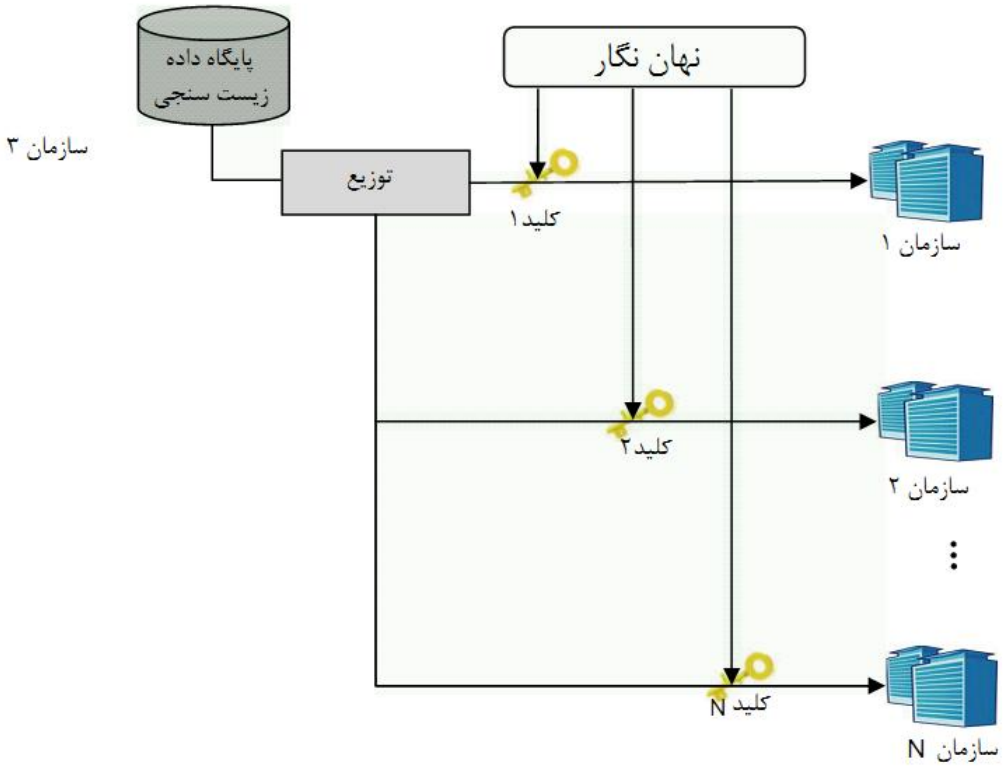
پس از ضبط یک نمونه زیست‌سنجی در طی فرآیند ثبت نام، یک نهان‌نگار زیست‌سنجی می‌تواند درون نمونه زیست‌سنجی تعبیه شده، و سپس آن نمونه زیست‌سنجی نهان‌نگاری‌شده می‌تواند در پایگاه داده ثبت نام ذخیره شود. با بررسی نهان‌نگار استخراج شده در هنگام بازیابی نمونه زیست‌سنجی از پایگاه داده ثبت نام، می‌توان به سرعت ثبت‌نام اطلاعات زیست‌سنجی غیرقانونی را که نهان‌نگار نادرست دارند، یا اصلا نهان‌نگار ندارند کشف کرد.

- شناسایی منبع توزیع نمونه‌های زیست‌سنجی فاش‌شده

اگر در هنگام به‌دست آوردن نمونه زیست‌سنجی، اطلاعات مربوط به فرد مسئول به عنوان یک نهان‌نگار زیست‌سنجی در آن تعبیه شود، درهنگام وقوع هرگونه افشای غیر قانونی از یک نمونه زیست‌سنجی، منبع توزیع نمونه‌های زیست‌سنجی فاش شده قابل شناسایی می‌باشد.

- ردیابی سازمان‌های مسئول برای نمونه‌های زیست‌سنجی فاش شده

داده‌های زیست‌سنجی می‌توانند بر مبنای ضرورت اداری و قضایی محلی، بین چندین سازمان توزیع شوند. با این حال، توزیع نمونه‌های زیست‌سنجی، امکان افشای غیر قانونی را افزایش می‌دهد. بنابراین می‌توان قبل از توزیع نمونه‌های زیست سنجی به هر سازمان، همان‌گونه که در شکل ث.۲ نشان داده شده است، یک شناساگر سازمان یکتا را به عنوان یک نهان‌نگار زیست‌سنجی در آن‌ها تعبیه نمود.



شکل ث۲- ردیابی توزیع غیرقانونی با استفاده از نهان نگاری زیست‌سنجی

در حالتی که N منبع توزیع‌کننده وجود دارد که هر یک از آن‌ها دارای یک شناساگر به عنوان یک نهان‌نگار زیست‌سنجی هستند، اگر هر گونه تردیدی در مورد قانونی بودن یک نمونه زیست‌سنجی وجود داشته باشد، منبع افشا می‌تواند از روی نهان‌نگار استخراج شده شناسایی گردد.

کتاب‌نامه

[1] ITU-T X.1086, Telebiometrics protection procedures — Part 1: A guideline to technical and managerial countermeasures for biometric data security

[2] ISO 19092:2008, Financial services — Biometrics — Security framework

[3] ISO/IEC 19785-4, Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications

[4] Jain, A. K., Bolle, R., Pankanti, S. (Eds) "Personal Identification In a Networked Society", Kluwer (1999)

[5] Nanavati, S., Thieme, M., Nanavati,R. "Biometrics Identity Verification in a Networked World", Wiley (2002)

[6] EU Project FIDIS (Future of Identity in the Information Society): A study on PKI and biometrics; D3.2, 2005; www.fidis.net

[7] EU Project FIDIS (Future of Identity in the Information Society): Biometrics in identity management; D3.10; 2007; www.fidis.net

[8] US InterNational Committee for information technology standards, Study report on biometrics in e-authentication (INCITS M1/07-0185), version 1.0; www.incits.org

[9] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery

[10] ISO/IEC 9797 (all parts), Information technology — Security techniques — Message Authentication Codes (MACs)

[11] ISO/IEC 10116: Information technology — Security techniques — Modes of operation for an n-bit block cipher

[12] ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital signatures with appendix

[13] ISO/IEC 18033-2:2006, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers

[14] ISO/IEC 18033-3:2005, Information technology — Security techniques — Encryption algorithms —Part 3: Block ciphers1)

[15] ISO/IEC 18033-4:2005, Information technology — Security techniques — Encryption algorithms —Part 4: Stream ciphers

[16] ISO/IEC 19772, Information technology — Security techniques — Authenticated encryption

[17] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[18] ISO/IEC JTC1 /SC 37 Standing Document 11 (SD11)

[19] ISO/IEC TR 24714-1, Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance

[20] ISO/IEC 24761, Information technology — Security techniques — Authentication context for biometrics

۱- استاندارد ISO/IEC 18033-3:2005 حذف و استاندارد ISO/IEC 18033-3:2010 جایگزین آن شده است.

[21] Breebaart, J., C. Busch, Grave, J., Kindt, E. "A reference architecture for biometric template protection based on pseudo identities" in Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, September 11-12, 2008, LNI-Series (2008)
[22] Tuyls, P., Akkermans, A. H. M., Kevenaar, T. A. M., Schrijen, G. J., Bazen, A. M., Veldhuis, R. N. J. "Practical biometric authentication with template protection" in Audio and Video-based biometric person authentication, pages 436-449, Springer, Berlin, Germany (2005)
[23] Juels, A., Wattenberg, M. "A fuzzy commitment scheme" in ACM Conference on Computer and Communications Security, pages 28-36 (1999)
[24] Soutar, C., Roberge, D., Stoianov, A., Gilroy,R., Vijaya Kumar, B. V. K. "Biometric Encryption using image processing" in Proc. SPIE 3314, pages 178-188 (1998)
[25] Juels, A., Sudan, M. "A fuzzy vault scheme", Designs, codes and cryptography, vol. 38 (2) (February 2006), pages 237-257, Springer, The Netherlands
[26] Linnartz, J-P. M. G., Tuyls, P. "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates" in AVBPA, pages 393-402 (2003)
[27] Dodis., Y., Reyzin, L., Smith, A. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data" in Eurocrypt (2004)
[28] Bringer, J., Chabanne, H., Pointcheval, D., Tang, Q. "Extended private information retrieval and its application in biometrics authentications" in CANS (2007)
[29] Buhan, I., Doumen, J., Hartel, P., Veldhuis, R. N. J. "Embedding renewable cryptographic keys into continuous noisy data" in Information and communications security, 10th international conference ICICS, Birmingham, UK, 294-310 (2008)
[30] ISO/IEC 7816-4:2005, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange
[31] Ratha, N. K., Chikkerur, S., Connell, J. H., and Bolle, R. M. "Generating cancellable fingerprint templates" in IEEE trans. pattern analysis and machine intelligence, 29(4), pages 561-572 (2007)
[32] Nandakumar, K., Nagar, A., Jain, A. K. "Hardening fingerprint fuzzy vault using password" in Advances in biometrics, Lecture Notes in Computer Science volume 4642/2007, Springer, Berlin (2007)
[33] Ratha, N. K., Connell, J. H., Bolle, R. M. "Enhancing security and privacy in biometrics-based authentication systems" IBM Systems Journal, vol. 40(3), March 2001
[34] Cavoukian, A., Stoianov, A. "Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy" Whitepaper information and privacy commissioner, Ontario 2007
[35] ITU-T X.1088, Telebiometrics digital key framework (TDK) — A framework for biometric digital key generation and protection
[36] Sutcu, Y, Sencar, H.T., and Memon, N. "A secure biometric authentication scheme based on robust hashing," Proc. of ACM Multimedia and Security Workshop. New York, USA, 111-116 (2005)
[37] Teoh, A. B. J., Goh, A., and Ngo, D. C. L. "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," IEEE Trans. on Pattern Analysis and Machine Intelligence, 28(12), 1892-1901 (2006)
[38] GenKey. "System, portable device and method for digital authenticating, crypting and signing by generating short-lived cryptokeys," US Patent 2006/0198514A1

[39] T. E. Boult, W. J. Scheirer, R. Woodworth, “Revocable fingerprint biotokens: accuracy and security analysis” in Proc. IEEE Inter. Conf. on Comput. Vis. and Patt. Recog, USA, 2007
[40] Q. Li, Y. Sutcu, N. Memon, “Secure Sketch for Biometric Templates,” Advances in Cryptology — ASIACRYPT 2006
[41] B. Yang, C. Busch, P. Bours, and D. Gafurov, “Robust Minutiae Hash for Fingerprint Template Protection,” SPIE Media Forensics and Security, Electronic Imaging, Jan.17-21, San Jose, USA, 2010
[42] ISO/IEC 24787, Information technology — Identification cards — On-card biometric comparison
[43] ISO/IEC 19792, Information technology — Security techniques — Security evaluation of biometrics
[44] ISO/IEC 24760-1, Information technology — Security techniques — A framework for identity management
[45] ISO/IEC 29100, Information technology — Security techniques — Privacy framework
[46] ISO/IEC JTC 1/SC 37 Standing Document 2 — Harmonized Biometric Vocabulary