INSO

21216

1st.Edition

2016

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

استاندارد ملی ایران

۲۱۲۱۶

چاپ اول
۱۳۹۵

فناوری اطلاعات– فنون امنیتی– حفاظت اطلاعات زیست‌سنجشی

Information technology — Security techniques — Biometric information protection

ICS: 35. 030

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات– فنون امنیتی– حفاظت اطلاعات زیست‌سنجشی»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون اداره کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ویراستار:	
قسمتی، سیمین (کارشناسی ارشد مهندسی فناوری اطلاعات)	مشاور رئیس مرکز آپا دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات– فنون امنیتی– حفاظت اطلاعات زیست‌سنجشی» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و سی و هشتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات داده مورخ ۱۳۹۵/۰۷/۱۲ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 24745:2011, Information technology — Security techniques — Biometric information protection

مقدمه

همچنان که اینترنت به قسمتی فراگیر از زندگی روزانه تبدیل می‌شود، خدماتی متنوع به وسیله آن فراهم می‌گردد؛ مانند بانکداری اینترنتی، مراقبت‌های بهداشتی از دور و غیره. به‌منظور فراهم نمودن این خدمات به شیوه‌ای امن، نیاز به سازوکارهای اصالت‌سنجی بین موضوعات و خدمات در حال ارائه، حیاتی‌تر می‌گردد. بعضی از این سازوکارهای اصالت‌سنجی که قبلا توسعه یافته‌اند، شامل طرح‌های بر پایه‌ی نشانه، شماره شناسایی شخصی و تراکنش (PIN/TAN)، طرح‌های امضای رقمی (دیجیتالی) بر مبنای سامانه‌ی رمزنگاری کلید عمومی و طرح‌های اصالت‌سنجی با استفاده از فنون زیست‌سنجشی هستند.

زیست‌سنجی – شناسایی خودکار اشخاص بر اساس مشخصه‌های رفتاری و روانشناسی آن‌ها- از سن سرچشمه می‌گیرد و شامل فنون شناسایی برمبنای تصویر اثرانگشت، الگوهای صوتی، تصویر عنبیه، تصویر چهره و مانند آن است. هزینه‌ی فنون زیست‌سنجشی در حال کاهش و این در حالی است که قابلیت اطمینان در حال افزایش است و در حال حاضر هر دو به‌منظور استفاده به عنوان سازوکاری برای احزار هویت، قابل قبول و پایدار هستند.

احرازهویت زیست‌سنجشی بین حریم خصوصی و اصالت‌سنجی قابل اطمینان، اختلاف بالقوه‌ای را معرفی می‌کند. از طرفی، مشخصه‌های زیست‌سنجشی، خصوصیاتی غیرقابل تغییر و وابسته به شخص و قابل تمایز هستند. این پیوند اعتبار به آن فرد، تضمین قدرتمندی برای اصالت‌سنجی فراهم می‌کند. از طرف دیگر، این پیوند قدرتمند، در زمینه‌ی خود پیرامون استفاده از زیست‌سنجه‌ها، نگرانی‌هایی در مورد حریم خصوصی دارد، به‌گونه‌ای که فرآیند غیرقانونی داده‌های زیست‌سنجشی و چالش‌ها را برای امنیت سامانه‌های زیست-سنجشی مطرح می‌کند تا مانع لورفتن مراجع زیست‌سنجشی شود. راه‌حل معمول برای نقض[1] اعتبار اصالت-سنجی -به منظور تغییر دادن کلمه‌ی عبور یا صادر کردن نشانه جدید- عموما برای اصالت‌سنجی‌های زیست‌سنجشی در دسترس نیست؛ به دلیل اینکه تغییر مشخصه‌های زیست‌سنجشی که یا خصوصیات روانشناسی ذاتی هستند یا ویژگی‌های رفتاری اشخاص دشوار یا غیرممکن است. در نهایت، انگشت یا چشم دیگر می‌تواند بکار گرفته شود؛ اما این انتخاب‌ها معمولا محدود هستند. بنابراین، اقدامات متقابل مقتضی برای امن نگاه داشتن امنیت سامانه‌ی زیست‌سنجشی و حفظ حریم خصوصیِ موضوعات داده‌ای ضروری است.

سامانه‌های زیست‌سنجشی معمولا مرجع زیست‌سنجشی را به دیگر اطلاعات قابل‌شناسایی شخصی (PII) [2] برای اصالت‌سنجی افراد پیوند می‌دهند. در این مورد، الزاماتی برای کسب اطمینان از امنیت ثبت داده‌های شامل اطلاعات زیست‌سنجشی مورد نیاز است. پیوند فزاینده مراجع زیست‌سنجشی با PII دیگر و اشتراک‌گذاری اطلاعات زیست‌سنجشی در حوزه‌ی قضایی، کسب اطمینان از محافظت اطلاعات زیست-

[1] - Compromise
[2] - Personally Identifiable Information

سنجشی و کسب مطلوبیت با مقررات متنوع حریم خصوصی را برای سازمان‌ها بسیار دشوار می‌کند.

فناوری اطلاعات– فنون امنیتی– حفاظت اطلاعات زیست‌سنجشی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنما برای حفاظت اطلاعات زیست‌سنجشی تحت الزاماتی متفاوت برای حفظ محرمانگی[۱]، یکپارچگی[۲]، تجدیدپذیری[۳]/ابطال‌پذیری[۴] این اطلاعات در حین ذخیره‌سازی و انتقال است. به‌علاوه، این استاندارد الزامات و راهنماهایی را برای مدیریت امن و سازگار با حفظ حریم خصوصی[۵] اطلاعات زیست‌سنجشی و همچنین برای پردازش آن‌ها فراهم می‌کند.

این استاندارد موارد زیر را مشخص می‌کند:

- تحلیل[۶] تهدیدات و اقدامات متقابل ذاتی[۷] در الگوهای کاربردی سامانه زیست‌سنجشی
- الزامات امنیتی برای پیوند امن بین مرجع زیست‌سنجشی[۸] و مرجع شناسه
- الگوهای کاربردی سامانه زیست‌سنجشی با فرانامه[۹]های متفاوت برای ذخیره‌سازی و مقایسه مراجع زیست‌سنجشی و
- راهنمایی در مورد حفاظت از حریم خصوصی افراد در حین پردازش اطلاعات زیست‌سنجشی

این استاندارد شامل موارد کلی مدیریتی مرتبط با امنیت فیزیکی، امنیت محیطی و مدیریت کلید برای فنون رمزنگاشتی[۱۰] نیست.

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات با تعاریف زیر به‌کار می‌رود:

1 - Confidentiality
2 - Integrity
3 - Renewability
4 - Revocability
5 - Privacy-compliant
6 - Analysis
7 - Inherent
8 - Biometric reference
9 - Scenario
10 - Cryptographic

۱-۲

اصالت‌سنجی

authentication

فرایند برقراری سطح درک شده‌ی اطمینان از این که، هستار[1] مشخص یا شناسه ادعا شده واقعی باشد.

یادآوری ۱- اصالت‌سنجی، شامل فرایند معلوم کردن یک سطح درک شده‌ی اطمینان از درستیِ شناسه ادعا شده است، قبل از اینکه هستار بتواند در یک حوزه ثبت و شناسایی شود.

یادآوری ۲- اگرچه این تعریف عمومی است اما کاربرد آن در این استاندارد محدود به اصالت‌سنجی زیست‌سنجشی موضوعات انسانی است.

[ISO 19092:2008]

۲-۲

داده کمکی

auxiliary data (AD)

داده وابسته به یک موضوع که بخشی از یک مرجع زیست‌سنجشی تجدیدپذیر است و ممکن است برای بازسازی شناسانه‌های دارای تخلص[2] در طی درستی سنجی یا به طور کلی برای درستی سنجی نیاز باشد.

یادآوری ۱- اگر داده کمکی بخشی از مرجع زیست‌سنجشی تجدیدپذیر[3] باشد، نیاز به ذخیره‌سازی در مکان مشابه با شناسانه-های دارای تخلص ندارد.

یادآوری ۲- ممکن است داده کمکی حاوی عناصر داده‌ای برای تنوع‌بخشی[4] باشد (به عنوان مثال، داده‌های تنوع‌بخشی)

یادآوری ۳- داده کمکی، عنصر مقایسه در طی درستی سنجیِ مرجع زیست‌سنجشی نیست.

یادآوری ۴- داده کمکی توسط سامانه زیست‌سنجشی در طی ثبت[5] تولید می‌شود.

مثال: عدد محرمانه رمزگذاری‌شده توسط یک کلید مشتق‌شده از یک نمونه زیست‌سنجشی که از رویکرد داده کمک کننده[6]، طرح‌واره[7] الزام فازی یا جهش فازی[8] استفاده می‌کند. برای مثال‌های عینی از PI و AD (این اختصارات در بند ۳، کوته‌نوشت‌ها، آمده است)، به پیوست ت، جدول ت-۱ مراجعه شود.

1 - Entity
2 - Pseudonymous
3 - Renewable
4 - Diversification
5 - Enrolment
6 - Helper data approach
7 - Scheme
8 - Fuzzy vault

۳-۲

مشخصه زیست‌سنجشی

biometric characteristic

مشخصه کاراندام‌شناختی[1] یا رفتاری یک فرد که می‌تواند شناسایی شود و از روی آن‌چه که شناسایی می‌شود، خصیصه[2]های زیست‌سنجشی تکرارپذیر می‌تواند برای اهداف تشخیص خودکار اشخاص استخراج شود.

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

۴-۲

داده زیست‌سنجشی

biometric data

نمونه[3] زیست‌سنجشی، خصیصه زیست‌سنجشی[4]، الگوی زیست‌سنجشی، ویژگی[5] زیست‌سنجشی و سایر اطلاعات توصیفی برای مشخصه‌های زیست‌سنجشی اصلی یا تجمیع اطلاعات بالا است.

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

۵-۲

موضوع داده‌های زیست‌سنجشی (موضوع)

biometric data subject (subject)

فردی که مرجع زیست‌سنجشی او درون سامانه زیست‌سنجشی است.

۶-۲

خصیصه زیست‌سنجشی

biometric feature

اعداد یا برچسب‌های استخراج‌شده از نمونه‌های زیست‌سنجشی و استفاده‌شده برای مقایسه است.

[ISO / IEC JTC 1/SC 37SD2 (V-11)]

---

1 - Physiological
2 - Feature
3 - Sample
4 - Biometric feature
5 - Property

۷-۲

حریم خصوصی اطلاعات زیست‌سنجشی

biometric information privacy

حق واپایشِ جمع‌آوری، انتقال، استفاده، ذخیره‌سازی و بایگانی کردن، امحا[1] و تجدید اطلاعات زیست-سنجشی یک فرد در کل چرخه زندگی خود است.

۸-۲

الگوی زیست‌سنجشی

biometric model

کارکرد ذخیره‌شده (وابسته به موضوع داده زیست‌سنجشی) که از یک خصیصه یا خصیصه‌های زیست-سنجشی تولیدشده از.

یادآوری – مقایسه، کارکرد ذخیره‌شده را در خصیصه‌های زیست‌سنجشی یک نمونه زیست‌سنجشی کاوشگر[2] به کار می‌برد تا امتیاز مقایسه را نتیجه دهد.

مثال: مثال کارکردهای ذخیره‌شده شامل الگوهای پنهان مارکف[3]، الگوهای ترکیبی گاووسی[4] یا شبکه‌های عصبی مصنوعی[5] است.

[ISO / IEC JTC 1/SC 37SD2 (V-11)]

۹-۲

ویژگی زیست‌سنجشی

biometric property

خواص توصیفی موضوع داده‌های زیست‌سنجشی که تخمین زده شده یا از نمونه زیست‌سنجشی توسط وسایل خودکار مشتق‌شده است.

مثال: اثرانگشت‌ها می‌تواند با توجه به ویژگی‌های زیست‌سنجشی خطوط اثر انگشت[6] جریان طبقه‌بندی شوند. (به‌طور مثال، انواع کمان، حلقه و چرخ)؛ تصاویر چهره می‌توانند برای تخمین سن یا جنسیت استفاده شوند.

[ISO / IEC JTC 1/SC 37SD2 (V-11)]

---

1 - Disposal
2 - Probe
3 - Hidden Markov Models
4 - Gaussian Mixture Models
5 - Artificial Neural Networks
6 - Ridge-flow

۱۰-۲

مرجع زیست‌سنجشی

biometric reference (BR)

یک یا چند نمونه زیست‌سنجشی، قالب‌های زیست‌سنجشی یا الگوهای زیست‌سنجشی ذخیره‌شده که به موضوع داده‌ای زیست‌سنجشی نسبت داده می‌شوند و در مقایسه به کار می‌روند.

یادآوری – به مرجع زیست‌سنجشی‌ای که می‌تواند تجدید شود، مرجع زیست‌سنجشی تجدیدپذیر گفته می‌شود.

مثال: تصویر چهره در گذرنامه، قالب جزئیات اثرانگشت در کارت شناسایی ملی، الگوی ترکیبی گاووسی، برای تشخیص سخنگو در دادگان[1].

[ISO / IEC JTC 1/SC 37SD2 (V-11)]

۱۱-۲

نمونه زیست‌سنجشی

biometric sample

نمایش قیاسی[2] یا رقمی[3] مشخصه‌های زیست‌سنجشی به دست آمده از یک افزاره اخذ زیست‌سنجشی یا زیرسامانه اخذ زیست‌سنجشی مقدم بر استخراج این خصیصه‌ها است.

[ISO / IEC JTC 1/SC 37SD2 (V-11)]

۱۲-۲

سامانه زیست‌سنجشی

biometric system

سامانه‌ای برای اهداف شناسایی خودکار اشخاص بر اساس مشخصه‌های رفتاری و کاراندام‌شناختی آن ها است.

۱۳-۲

قالب زیست‌سنجشی

biometric template

مجموعه خصیصه‌های زیست‌سنجشی ذخیره‌شده که به‌طور مستقیم با خصیصه‌های زیست‌سنجشی کاوشگر

1 - Database
2 - Analog
3 - Digital

قابل‌مقایسه است.

۱۴-۲

ادعا

claim

اظهار شناسه است.

۱۵-۲

مدعی

claimant

فردی که ادعای شناسه دارد.

یادآوری- ادعاها می‌توانند به روش‌های متعددی درستی‌سنجی شوند که ممکن است برخی از آن ها بر اساس زیست‌سنجی باشند.

۱۶-۲

شناسانه عام

common identifier

شناسانه‌ای که برای وابستگی مراجع شناسه و مراجع زیست‌سنجشی در دادگان مجزای فیزیکی یا منطقی است.

۱۷-۲

تنوع‌بخشی

diversification

ایجاد عمدی مراجع زیست‌سنجشی چندگانه، مستقل و تغییر شکل یافته از یک یا چند نمونه زیست‌سنجشی به دست آمده از یک مبحث داده برای اهداف افزایش امنیت و حریم خصوصی.

۱۸-۲

شناسایی

identification

فرایند (زیست‌سنجشی) انجام جستجوی زیست‌سنجشی در یک دادگان ثبت‌نام، برای پیدا کردن و بازگرداندن مرجع شناسه قابل استناد به یک فرد واحد است.

۱۹-۲

شناسانه

identifier

یک یا چند خواص که به‌طور منحصر به فرد یک هستار را در یک حوزه معین مشخص می‌کند.

مثال: نام یک باشگاه با شماره عضویت باشگاه، شماره کارت بیمه سلامت همراه با نام شرکت بیمه، یک آدرس IP و شناسانه منحصر به فرد جهانی[1].

۲۰-۲

شناسه

identity

مجموعه‌ای از ویژگی‌ها و مشخصه‌های یک هستار که می‌تواند برای توصیف وضعیت، ظاهر و یا سایر کیفیت‌های آن استفاده شود.

۲۱-۲

سامانه مدیریت شناسه

identity management system (IdMS)

سامانه‌ای که اطلاعات شناسه هستار را در سراسر چرخه زندگی اطلاعات در یک حوزه واپایش می‌کند.

۲۲-۲

مرجع شناسه

identity reference (IR)

خواص غیرزیست‌سنجشی که شناسانه‌ای است با مقداری که برای طول مدت وجود هستار در یک حوزه به همان شکل باقی می‌ماند.

۲۳-۲

بازگشت‌ناپذیری

irreversibility

ویژگی یک تغییرشکل که در آن، یک مرجع زیست‌سنجشی را از نمونه(های) یا خصیصه‌های زیست‌سنجشی

1 - Universal unique identifier

ایجاد می‌کند، طوری که دانش مرجع زیست‌سنجشی تغییر شکل یافته، نمی‌تواند برای تعیین اطلاعاتی راجع به تولید خصیصه‌ها یا نمونه‌های زیست‌سنجشی استفاده شود.

۲۴-۲

اطلاعات قابل شناسایی شخصی

personally identifiable information (PII)

هر اطلاعاتی،

- که شناسایی شود یا بتواند در شناسایی، تماس و یا مکان‌یابی یک فرد با اطلاعات مربوط استفاده شود.
- از هر اطلاعات تعیین شناسه یا تماس یک فرد بتواند مشتق شود و یا
- که ممکن است مستقیم یا غیرمستقیم به یک فرد عادی پیوند داده شود.

[ISO / IEC 29100:-]

۲۵-۲

شناسانه‌ی دارای تخلص

pseudonymous identifier (PI)

بخشی از مرجع زیست‌سنجشی تجدیدپذیر که نشان دهنده‌ی یک موضوع داده‌ای یا فردی درون حوزه معین به‌وسیله شناسه حفاظت شده است. این شناسه می‌تواند به‌وسیله نمونه زیست‌سنجشی اخذشده و داده کمکی (در صورت امکان) درستی‌سنجی شود.

یادآوری ۱- شناسانه‌ی دارای تخلص شامل هیچ‌گونه اطلاعاتی که امکان بازیابی نمونه زیست‌سنجشی اصلی، خصیصه‌های زیست‌سنجشی اصلی یا شناسه واقعی دارنده‌اش را در اختیار قرار دهد، نیست.

یادآوری ۲- شناسانه‌ی دارای تخلص در خارج از حوزه خدمات بی‌معنا است.

یادآوری ۳- داده‌ی زیست‌سنجشی رمزگذاری‌شده با یک رمز که امکان بازیابی داده متن اصلی[1] را بدهد، شناسانه‌ی دارای تخلص نیست.

یادآوری ۴- شناسانه‌ی دارای تخلص عنصر مقایسه در حین درستی‌سنجی مرجع زیست‌سنجشی است.

یادآوری ۵- برای مثال‌هایی از PI و AD به پیوست ت و جدول ت-۱ مراجعه شود.

1 - Plain-text

۲۶-۲

کُدبند شناسانه‌ی دارای تخلص

pseudonymous identifier encoder (PIE)

سامانه، فرایند یا الگوریتمی است که مرجع زیست‌سنجشی تجدیدپذیر حاوی شناسانه‌ی دارای تخلص (PI) و داده‌های کمکی ممکن (AD) بر اساس نمونه زیست‌سنجشی یا قالب زیست‌سنجشی را تولید می‌کند.

۲۷-۲

تجدیدپذیری

renewability

ویژگی یک تغییر شکل یا فرایند ایجاد مرجع زیست‌سنجشی چندگانه، مستقل و تغییر شکل یافته که از یک یا چند نمونه زیست‌سنجشی مشتق می‌شود است. این مرجع زیست‌سنجشی از موضوع داده مشابه به دست می‌آید و می‌تواند در شناسایی شخص استفاده شود در حالی که اطلاعاتی راجع به مرجع اصلی آشکار نمی‌شود.

۲۸-۲

مرجع زیست‌سنجشی تجدیدپذیر

renewable biometric reference

شناسانه‌ی ابطال‌پذیر یا تجدیدپذیر است که موضوع داده یا فردی در حوزه معین به‌وسیله شناسه یگانه حفاظت شده و ساخته شده از نمونه زیست‌سنجشی اخذشده را ارائه می‌دهد.

یادآوری - یک مرجع زیست‌سنجشی تجدیدپذیر حاوی شناسانه‌ی دارای تخلص و عناصر داده اضافی و انتخابی مورد نیاز برای بازبینی یا شناسایی زیست‌سنجشی مثل داده کمکی است.

۲۹-۲

ابطال‌پذیری

revocability

توانایی جلوگیری از درستی‌سنجی موفق آتی یک مرجع زیست‌سنجشی معین و مرجع شناسه مربوط به آن است.

یادآوری– عدم پذیرش یک هستار ممکن است بر اساس ظهور آن در فهرست ابطال رخ دهد.

۳۰-۲

کانال امن

secure channel

کانال ارتباطی که محرمانگی و یکپارچگی پیام‌های مبادله شده را تامین می‌کند.

۳۱-۲

نمودافزار

token

افزاره فیزیکی که مرجع زیست‌سنجشی را ذخیره می‌کند و در برخی موارد، مقایسه زیست‌سنجشی درونی[1] را اجرا می‌نماید.

مثال: کارت هوشمند[2]، حافظه USB یا تراشه RFID در گذرنامه الکترونیکی.

۳۲-۲

پیوند ناپذیری

unlinkability

ویژگی دو یا چند مرجع زیست‌سنجشی که نمی‌توانند به هم‌دیگر و یا به موضوع(ها)ی که از آن مشتق شده‌اند، پیوند داده شوند.

۳۳-۲

درستی سنجی

verification

فرایند (زیست‌سنجشی) تایید ادعا، به این معنی که فردی که موضوع فرایند اخذ زیست‌سنجشی است همان منبعِ مرجع شناسه ادعا شده است.

۳ کوته‌نوشت‌ها

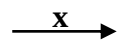
AD Auxiliary Data داده کمکی

1 - On-board
2 - Smart card

AFIS	Automated Fingerprint Identification Systems	سامانه‌های شناسایی اثرانگشت خودکار
BR	Biometric Reference	مرجع زیست‌سنجشی
BIR	Biometric Information Record	ثبت اطلاعات زیست‌سنجشی
CI	Common Identifier	شناسانه عام
OCC	On-Card Comparison	مقایسه درون کارت
DB_{BR}	Database containing Biometric Reference	دادگان حاوی مرجع زیست‌سنجشی
DB_{IR}	Database containing Identity Reference	دادگان حاوی مرجع شناسه
IdMS	Identity Management System	سامانه مدیریت شناسه
IR	Identity Reference	مرجع شناسه
MAC	Message Authentication Code	کد اصالت‌سنجی پیام
PDA	Personal Digital Assistant	دستیار رقمی شخص
PET	Privacy Enhancing Technology	فناوری ارتقای حریم خصوصی
PI	Pseudonymous Identifier	شناسانه‌ی دارای تخلص
PIC	Pseudonymous Identifier Comparator	مقایسه کننده شناسانه‌ی دارای تخلص
PIE	Pseudonymous Identifier Encoder	کدبند شناسانه‌ی دارای تخلص
PII	Personally Identifiable Information	اطلاعات قابل شناسایی شخصی
PIR	Pseudonymous Identifier Recoder	ثبت‌کننده شناسانه‌ی دارای تخلص
RBR	Renewable Biometric Reference	مرجع زیست‌سنجشی تجدیدپذیر
RFID	Radio Frequency Identification	شناسایی بسامد رادیویی
TTP	Trusted Third Party	شخص سوم مورد اعتماد

USB Universal Serial Bus همه‌گذر

UUID Universal Unique Identifier شناسانه منحصر به فرد جهانی



پیکانی که جریان اطلاعات ساده داده x را نمایش می‌دهد یا راه‌اندازی پروتکلِ تعاملی که داده‌های مبادله شده آن می‌تواند بستگی به تمام یا بخشی از x داشته باشد.

یادآوری ۱- هرگاه یک سامانه پیام‌رسان امن مثل ISO/IEC 7816-4 استفاده شود، x ممکن است رمزگذاری‌شده باشد.

یادآوری ۲- هرگاه، به عنوان مثال، فن دانش-صفر[1] استفاده شود ممکن است پروتکل تعاملی هیچ‌گونه اطلاعاتی از x را انتقال ندهد.

۴ سامانه‌های زیست‌سنجشی

۴-۱ مقدمه‌ای بر سامانه‌های زیست‌سنجشی

سامانه‌های زیست‌سنجشی تشخیص خودکار اشخاص را بر اساس یک یا چند مشخصه کاراندام‌شناختی (ویژگی‌های فیزیکی بدن مثل اثرانگشت) و یا رفتاری (کاری که اشخاص انجام می‌دهند مثل راه رفتن) انجام می‌دهد.

مشخصه‌های کاراندام‌شناختی شامل موارد زیر هستند اما محدود به آن‌ها نمی‌شوند:

- اثرانگشت
- چهره
- عنبیه
- هندسه دست
- سیاهرگ دست و انگشت
- شبکیه چشم
- DNA و
- اثر کف دست انسان

و مشخصه‌های رفتاری شامل موارد زیر می‌شوند اما محدود به آن نیستند.

1 - Zero-knowledge technique

- امضا
- گام برداشتن و
- صدا

موارد زیر ویژگی‌های مطلوب مشخصه‌های زیست‌سنجشی است که منجر به تمـایز موضـوع خـوب و کـارایی تشخیص قابل‌اطمینان می‌شود [۴]:

- جامعیت[۱]: بهتر است هر فردی مشخصه داشته باشد.
- یکتایی[۲]: بهتر است هر فردی مشخصه قابل تشخیص داشته باشد.
- ماندگاری[۳]: بهتر است مشخصه‌ها با گذشت زمان مغایرت نشان ندهند.
- قابلیت جمع‌آوری[۴]: بهتر است مشخصه‌ها به سادگی از مباحث جمع‌آوری شوند.
- قابلیت تکرار: بهتر است مشخصه‌ها به اندازه کافی متمایز و قابل تکرار باشند تا به تشخیص موفقی از موضوع دست یابند.

از نقطه نظر کاربرد، ویژگی‌های اضافی زیر باید به حساب آیند.

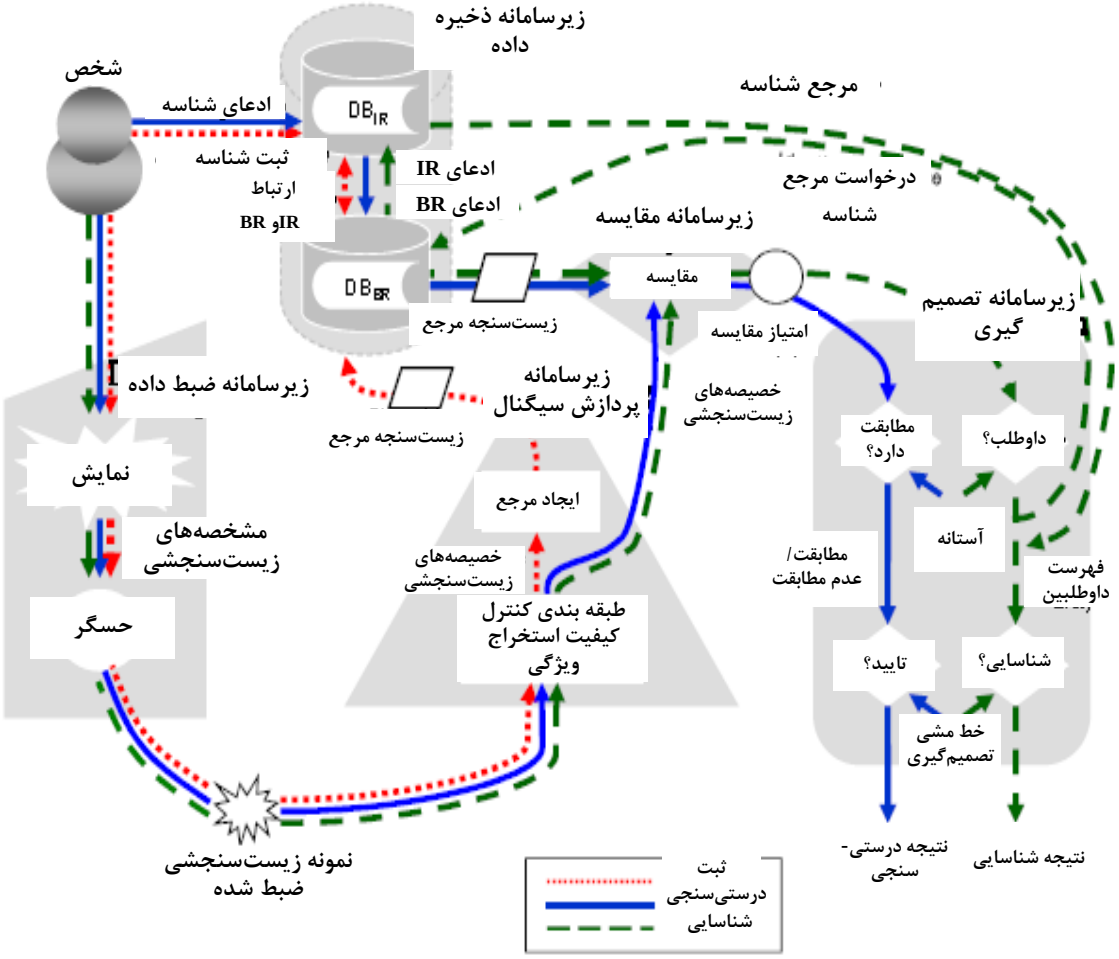
- عملکرد، که اساسا مربوط به نرخ موفقیت در تشخیص اشخاص است.
- قابل‌قبول بودن، که سطح تمایل را به‌وسیله موضوعی که سامانه زیست‌سنجشی را استفاده مـی‌کنـد ارائه می‌دهد و
- مقاومت در برابر کلاه‌برداری[۵]، که نشان می‌دهد استفاده از المثنی مشخصه زیست‌سنجشی برای گیر انداختن سامانه زیست‌سنجشی چقدر سخت است.

برای شناسایی و درستی سنجی یک فرد، سامانه زیست‌سنجشی یک یا چند نمونـه آشـکارگر بـرای مقایسـه مراجع زیست‌سنجشی ذخیره‌شده را پردازش می‌کند. مرجع زیست‌سنجشی می‌تواند نمونـه زیسـت‌سنجشـی (به عنوان مثال: یک تصویر که مشخصه زیست‌سنجشی را ارائه می‌دهد) یا مجموعـه مشخصـه‌هـای زیسـت-سنجشی (به عنوان مثال: یک قالب که از تصویر مشتق‌شده) باشد و یا می‌تواند یک الگـوی زیسـت‌سنجشـی باشد که از مشخصه‌ها ساخته می‌شود.

مخصوصاً، خصیصه‌های زیست‌سنجشی کاراندام‌شناختی به‌سختی تغییـر مـی‌کننـد و بنـابراین نقـض[۶] آن‌هـا می‌تواند نتایج پایداری برای شخص در کاربردهایی که در آن ثبات خصیصه‌ها فرض شده است، داشته باشد.

1 - Universality
2 - Uniqueness
3 - Permanence
4 - Collectability
5 - Spoof resistance
6 - Compromise

۲-۴ عملکردهای سامانه زیست‌سنجشی



شکل ۱- ساختار مفهومی سامانه زیست‌سنجشی

عملکرد کلی سامانه زیست‌سنجشی در شکل ۱ نمایش داده شده است که نسخه گسترش‌یافته از شکل اصلی در استاندارد ISO/IEC SC 37 SD11 است و پردازش مرجع شناسه را برجسته می‌کند.

اغلب سامانه زیست‌سنجشی حاوی پنج زیرسامانه است:

- یک زیرسامانه اخذ داده زیست‌سنجشی، که شامل افزاره‌های اخذ زیست‌سنجشی یا حسگرهایی برای جمع‌آوری سیگنال‌ها از یک مشخصه زیست‌سنجشی و تبدیل آن ها به نمونه زیست‌سنجشی مثل تصویر اثرانگشت، تصویر چهره یا اخذ صدا است.
- یک زیرسامانه پردازش سیگنال، که خصیصه‌های زیست‌سنجشی را از یک نمونه زیست‌سنجشی با هدف خارج کردن اعداد و برچسب‌هایی که با موارد خارج شده از سایر نمونه‌های زیست‌سنجشی

مقایسه می‌شوند، استخراج می‌کند. در اینجا خصیصه زیست‌سنجشی استخراج‌شده از فرایند شناسایی و درستی سنجی ذخیره می‌شود.

- یک زیرسامانه ذخیره داده، که در ابتدا هر جا انقیاد مراجع زیست‌سنجشی ثبت‌شده به مرجع شناسه رخ دهد، به عنوان یک دادگان ثبت، انجام وظیفه می‌کند. ممکن است داده حاوی داده زیست-سنجشی و همچنین داده غیر زیست‌سنجشی مثل مرجع شناسه مربوط به موضوع باشد. در واقع DB_{IR} و DB_{BR} اغلب برای دلایل امنیتی و خط حریم خصوصی به‌طور منطقی و فیزیکی جدا شده‌اند. توضیحات بیشتر DB_{IR} پیوند داده شده با DB_{BR} در پیوست الف آمده است.

- یک زیرسامانه مقایسه، که شباهت بین نمونه‌های زیست‌سنجشی اخذشده (یا خصیصه‌های مشتق-شده) و مراجع زیست‌سنجشی ذخیره‌شده را معین می‌کند. در مورد مقایسه تک‌به‌تک استفاده‌شده در فرایند درستی سنجی، یک نمونه زیست‌سنجشی اخذشده با مرجع زیست‌سنجشی اخذشده از یک موضوع داده زیست‌سنجشی مقایسه می‌شود تا امتیاز مقایسه تولید شود. به هر حال در مقایسه یک به چند استفاده‌شده در فرایند شناسایی، یک خصیصه استخراج‌شده از موضوع داده زیست-سنجشی در برابر مجموعه‌ای از مراجع زیست‌سنجشی بیش از یک موضوع داده زیست‌سنجشی مقایسه می‌شود تا مجموعه امتیازات مقایسه بازگردانده شود.

- یک زیرسامانه تصمیم‌گیری، که تعیین می‌کند که آیا نمونه زیست‌سنجشی اخذشده و مرجع زیست-سنجشی یک منبع مشابه (موضوع زیست‌سنجشی) بر اساس امتیازات مقایسه و خط‌مشی تصمیم‌گیری شامل یک آستانه دارند. در مورد فرایند درستی سنجی، ممکن است موضوع داده زیست‌سنجشی بر طبق امتیاز مقایسه رد یا پذیرفته شود. در مورد شناسایی، فهرست شناسه‌های داوطلب که خط‌مشی تصمیم‌گیری را برآورده می‌کند، ارائه شده است.

در ماهیت، یک سامانه زیست‌سنجشی سه فرایند کاربردی اصلی را وارد می‌کند:

- فرایند ثبت: ایجاد و ذخیره یک گزارش داده ثبت برای یک فرد که موضوع فرایند اخذ زیست-سنجشی در تطابق با خط‌مشی ثبت است. معمولا موضوع، مشخصه‌های زیست‌سنجشی خود را به همراه مرجع شناسه خود به حسگر ارائه می‌دهد. نمونه زیست‌سنجشی اخذشده برای استخراج خصیصه‌هایی که به عنوان مرجع در بانک داده ثبت با مرجع شناسه ثبت‌شده است، پردازش می‌شود.

- فرایند شناسایی: جستجو دادگان ثبت‌شده در برابر خصیصه‌های زیست‌سنجشی اخذ و استخراج‌شده برای بازگرداندن فهرست داوطلب. فهرست داوطلب شامل اشخاصی است که مراجع آن ها مطابق با خصیصه در زیرسامانه‌های مقایسه است و مشابهت، ارزش امتیاز بیشتر از ارزش آستانه از پیش معرفی شده دارد.

- فرایند درستی سنجی: آزمودن یک ادعا شخصی که موضوع فرایند اخذ زیست‌سنجشی است، منبع مرجع زیست‌سنجشی تعیین‌شده است. موضوع، مرجع شناسه‌اش برای ادعای شناسه و همچنین

مشخصه‌های زیست‌سنجشی خود در افزاره اخذ را ارائه می‌دهد. این افزاره نمونه‌های زیست‌سنجشی استفاده‌شده را در مقایسه با مرجع زیست‌سنجشی پیوند داده شده با مرجع شناسه برای شناسه ادعا شده نیاز دارد.

از آن جایی که فرایند درستی سنجی هم مرجع زیست‌سنجشی و هم مرجع شناسه را نیاز دارد، این فرایند می‌تواند بر اطلاعات حریم خصوصی اثر بگذارد. فرایند شناسایی نیاز به جستجو جامع دادگان ثبت دارد؛ بنابراین می‌تواند روی حریم خصوصی فیزیکی موضوع هم اثر بگذارد. به‌طور کل درستی سنجی دخالت کمتری نسبت به شناسایی در حریم خصوصی دارد.

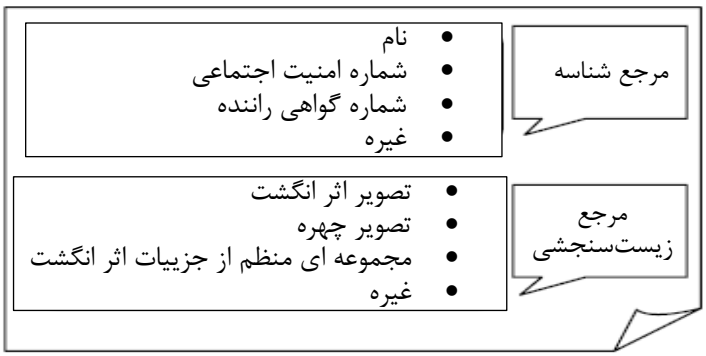
پنج زیرسامانه ذکر شده در بالا بلوک‌های کاربردی فناوری را ارائه می‌دهند که پردازش داده‌های زیست-سنجشی را اخذ، ذخیره، مقایسه و تصمیم‌گیری می‌کند. به‌علاوه سایر زیرسامانه‌های کاربردی می‌توانند شامل بندهای زیر باشند [۷].

- یک زیرسامانه انطباق مرجع، که با استفاده از خصیصه زیست‌سنجشی جدید، مرجع استخراج‌شده از فرایند درستی سنجی یا شناسایی موفق را اصلاح می‌کند. در کل انطباق توسط سامانه‌های زیست-سنجشی به کار گرفته می‌شود تا معیارهای بیرونی را بازتاب دهد و تاثیر آن ها در نرخ تشخیص را کمینه کند همچنین می‌تواند برای ضعیف کردن اثرات بالقوه کهنه شدن مرجع استفاده شود. انطباق نظارت نشده می‌تواند به‌طور خودکار بر اساس معیارهای کاربردی معین اجرا شود. به عنوان مثال، هرگاه امتیاز مقایسه زیست‌سنجشی بالا نباشد اما سایر معیارها به‌طور واضح شناسه ادعا شده را پشتیبانی کنند، می‌تواند فراخوانده شود. از آن جایی که امتیاز مقایسه کم ممکن است سبب شود که سامانه کاربر واقعی را رد کند، توصیه می‌شود انطباق سامانه انطباق مرجع در مراحل اولیه تاسیس سامانه زیست‌سنجشی در نظر گرفته شود.
- یک زیرسامانه حاکمیتی که خط‌مشی روی‌هم‌رفته، پیاده‌سازی و استفاده از سامانه زیست‌سنجشی را در تطابق با محدودیت‌های قانونی، در حوزه قضایی و وابسته به اجتماع و الزامات حریم خصوصی مرتبط را واپایش می‌کند. مثال‌های روشن‌کننده شامل موارد زیر هستند:
  - تدارک حریم خصوصی اطلاعات مرتبط با موضوع در مدت پردازش زیست‌سنجشی؛
  - ذخیره‌سازی و قالب‌بندی مراجع زیست‌سنجشی و داده‌های مبادله شده زیست-سنجشی؛
  - تصمیم‌گیری در مورد سازوکارهای امضای رقمی و رمزگذاری برای محرمانگی و یکپارچگی PII که شامل داده‌های زیست‌سنجشی است؛
  - تحلیل آسیب‌پذیری حملات امنیتی در برابر سامانه کلی زیست‌سنجشی و پیاده‌سازی اقدامات متقابل مناسب؛
  - تدارک داوری نهایی در مورد بازده تصمیمات و یا امتیازات؛

- کارگزاری ارزش‌های آستانه برای زیرسامانه تصمیم‌گیری؛
- واپایش محیط عملکردی و ذخیره داده غیر زیست‌سنجشی؛ و
- تدارک حفاظت مناسب برای حریم خصوصی موضوع

۳-۴ مراجع زیست‌سنجشی و مراجع شناسه

یک فرد در هر حوزه ویژه یک شناسانه دارد اما ممکن است مراجع شناسه متعددی این شخص را در آن حوزه شناسایی کند. هر مرجع شناسه یک صفت یا ترکیب چند صفت از شناسه یک وجود است که آن وجود را به‌طور منحصر به فرد در حوزه ویژه شناسایی می‌کند. همچنین یک مرجع شناسه می‌تواند ترکیب چند صفت از شخص باشد. مرجع زیست‌سنجشی یکی از چند صفت متعلق به شخص است که می‌تواند برای تشخیص آن شخص در حوزه استفاده شود. این استاندارد صفات شناسه را در دسته‌های غیر زیست‌سنجشی و زیست‌سنجشی طبقه‌بندی می‌کند. به منظور ساده‌سازی، دسته اول مربوط به مرجع شناسه (IR) و دسته دوم مربوط به مرجع زیست‌سنجشی (BR) است. برخی مثال‌ها از مراجع شناسه و مراجع زیست‌سنجشی که جامع یا فهرست قطعی نیستند، در شکل ۲ نمایش داده شده است. در اینجا مرجع اصلی مجموعه صفت‌های استفاده‌شده در شناسایی یک فرد را ارائه می‌دهد.

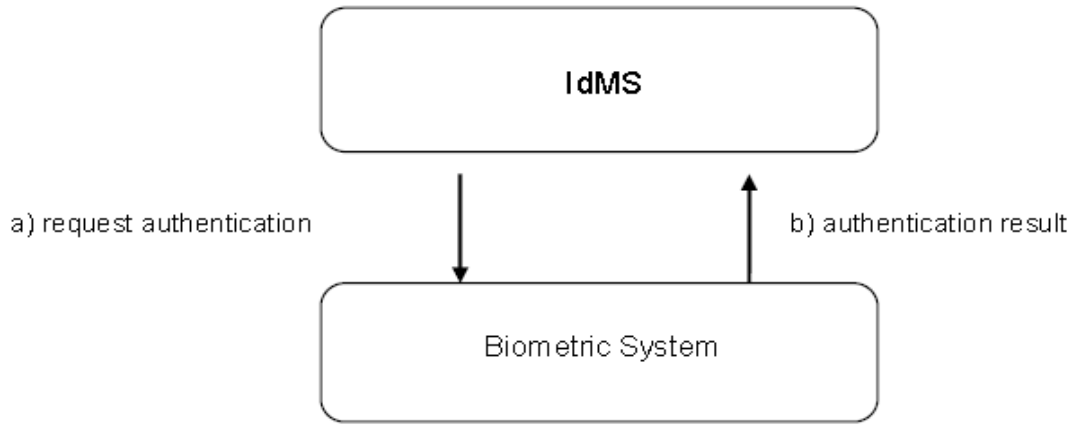


شکل ۲- مراجع شناسه و مراجع زیست‌سنجشی

۴-۴ سامانه‌های زیست‌سنجشی و سامانه‌های مدیریت شناسه

سامانه IdMS عملکرد مهمی در هر حوزه برای اجتناب از تضاد شناسه یا ابهامات دارد (برای جزئیات بیشتر در مورد IdMS به استاندارد ISO /IEC 24760-1 مراجعه شود)

یک سامانه اصالت‌سنجی نیاز به فرایند شناسایی و درستی سنجی دقیق در حوزه تعریف‌شده و رابطه تعریف‌شده با فرایندهای نام‌نویسی و ثبت در همان حوزه یا حوزه‌های دیگر دارد. IdMS ممکن است هرگاه زیست‌سنجی برای تامین خدمات اصالت‌سنجی استفاده شوند، نیاز به اصالت‌سنجی از سامانه زیست‌سنجشی دارد (الف در شکل ۳) و ممکن است سامانه زیست‌سنجشی نتیجه اصالت‌سنجی را برای IdMS تامین کند (ب در شکل ۳).



شکل ۳- سامانه زیست‌سنجشی به عنوان تامین کننده خدمات اصالت‌سنجی برای IdMS

۵-۴ اطلاعات قابل شناسایی شخصی و شناسانه‌های منحصر به فرد جهانی

برخی سامانه‌های زیست‌سنجشی از نمونه‌های زیست‌سنجشی مثل تصویر چهره در گذرنامه الکترونیکی استفاده می‌کنند تا شخص را مستقیماً شناسایی کنند. سایر سامانه‌ها از خصیصه‌های زیست‌سنجشی مثل جزئیات دقیق اثرانگشت و ضرایب مشترک بردارهای ویژه چهره برای شناسایی مستقیم شخص در محدوده مرجع شناسه استفاده می‌کنند. توانایی انقیاد داده‌های زیست‌سنجشی به موضوع منجر به ساخت مراجع زیست‌سنجشی PII می‌شود.

مراجع زیست‌سنجشی به دلیل ممتاز بودنشان، قابلیت استفاده شدن به عنوان شناسانه منحصر به فرد جهانی (UUID) را دارند. یک UUID مرجع شناسهی است که می‌تواند برای پیوند اطلاعات شخصی در بین دادگان مختلف استفاده شود، بنابراین منجر به یک تهدید بالقوه برای حریم خصوصی خواهد بود. همین‌طور، نگرانی‌های مهمی در مورد استفاده از مرجع زیست‌سنجشی به عنوان UUID بیان شده است. توصیه می‌شود مراجع زیست‌سنجشی به عنوان یک شناسانه منحصر به فرد جهانی استفاده نشوند، مگر در مواردی که نیاز واضحی به آن باشد.

UUID به یک مخاطره بالقوه برای حریم خصوصی تبدیل شده است که در آن یک فرد می‌تواند در بین دادگان حاوی PII متناظر پیگردی و پایشگری شود. هرگاه مرجع زیست‌سنجشی یا پیوند آن با مرجع شناسه استفاده شود، می‌تواند به عنوان اطلاعات قابل شناسایی شخصی طبقه‌بندی شود که ممکن است برای شخص در حوزه ویژه مهم باشد. اگر دادگان UUID از داده زیست‌سنجشی به کار گرفته شود، توصیه می‌شود ملاحظات در طرحی که الزامات ابطال‌پذیر و تجدیدپذیری برای محدود کردن مقایسه سرتاسری را تامین می‌کند، برآورده شود. به عنوان مثال، استفاده مراجع متنوع شده که در این استاندارد شرح داده شده‌اند.

۶-۴ ملاحظات اجتماعی

کاربرد سامانه‌های زیست‌سنجشی همواره جنبه‌های اجتماعی دارد، جنبه‌هایی که ممکن است در الزامات قانونی مربوط به عملکرد این گونه سامانه‌ها (مثل آن‌هایی که مربوط به حفاظت داده‌های شخصی هستند) مدون شوند، در حالی که سایر جنبه‌ها مثل قابلیت پذیرش توسط مباحث که از این سامانه‌ها استفاده می‌کنند، بسیار مطلوب هستند و به عملکرد خوب سامانه کمک خواهند کرد. قابلیت پذیرش یک سامانه ممکن است توسط معیارهای مذهبی، نژادی و فرهنگی و همچنین ویژگی‌های کاراندام‌شناختی شخصی تحت تاثیر قرار گیرد.

در تمام استقرارهای سامانه‌های زیست‌سنجشی، توصیه می‌شود آن اشخاص و سازمان‌هایی که مسئول عملکردشان هستند تشخیص دهند که حفاظت از داده‌های زیست‌سنجشی به‌وسیله راهکارهای امنیتی مناسب برای برآوردن الزامات قانونی (برای حفاظت داده‌های شخصی) و همچنین کمک به پذیرش آن‌ها توسط اجتماع و اشخاص ضروری است.

به روش مشابه، توصیه می‌شود طراحان و اجراکنندگان سامانه‌های استفاده‌کننده از زیست‌سنجی، اطمینان یابند که تعهدات قانونی[1] و عملکرد خوب در ارتباط با بندهای زیر مشاهده شود:

- بهداشت و امنیت
- پذیرش که اطمینان یابد سامانه‌ها باوجود تلاش‌های کم فیزیکی و دانشی به‌وسیله گسترده‌ترین جمعیت ممکن بخصوص برای مباحث از کار افتاده قابل استفاده باشند.
- قابلیت استفاده که سامانه‌هایی را ارائه می‌کند که در عمل مؤثر، کارآمد و راضی‌کننده هستند.

برای بحث بیشتر در مورد ملاحظات اجتماعی و متقابل قضایی[2] در کاربردهای تجاری به گزارش فنی ISO/IEC TR 24714-1 مراجعه شود.

۵ جنبه‌های امنیتی یک سامانه زیست‌سنجشی

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

۵-۱-۱ محرمانگی

محرمانگی یک ویژگی است که از اطلاعات در برابر دسترسی‌های غیرمجاز یا افشاگری‌ها محافظت می‌کند. در سامانه‌های زیست‌سنجشی یک مرجع زیست‌سنجشی در طی فرایند ثبت در دادگان مرجع زیست-سنجشی ذخیره‌شده است، در طی فرایند شناسایی و درستی سنجی به زیرسامانه مقایسه منتقل می‌شود.

1 - Legal obligations
2 - Societal and cross-jurisdictional

در طی فرایند، ممکن است مرجع زیست‌سنجشی در دسترس نهادهای غیرمجاز قرار گیرد و ممکن است خوانده شود و یا پیوند آن با اطلاعات شناسه قطع گردد. افشاگری‌های غیرمجاز اطلاعات ممکن است منجر به تهدیدهای حیاتی حریم خصوصی شود زیرا سنجه‌های زیست‌سنجشی حساس هستند. محرمانگی داده‌های زیست‌سنجشی ذخیره و منتقل شده می‌تواند از راه‌کارهای واپایش دسترسی و اشکال مختلف فناوری‌های رمزگذاری به دست آید.

یادآوری- اشکال مختلف الگوریتم‌های رمزگذاری، اعم از رمزگذاری متقارن یا غیرمتقارن می‌تواند برای تامین محرمانگی داده‌ها استفاده شود. برای اطلاعات بیشتر به پیوست ب-۱ مراجعه شود.

۵-۱-۲ یکپارچگی

یکپارچگی ویژگی تامین کردن دقت و تمامیت دارایی‌ها است. یکپارچگی مرجع زیست‌سنجشی برای اطمینان از امنیت سامانه زیست‌سنجشی حیاتی است. یکپارچگی فرایند اصالت‌سنجی بستگی به یکپارچگی مرجع زیست‌سنجشی دارد. اگر هم مرجع زیست‌سنجشی و هم ویژگی زیست‌سنجشی اخذ و استخراج‌شده غیرقابل‌اعتماد باشند، اصالت‌سنجی نتیجه شده هم غیرقابل‌اعتماد خواهد بود. مراجع یا نمونه‌های زیست-سنجشی غیرقابل‌اعتماد می‌توانند برای یک یا چند مورد از دلایل زیر رخ دهند:

- انحراف تصادفی به دلیل عمل کردن نامناسب سخت‌افزار یا نرم‌افزار
- اصلاح تصادفی یا عمدی مرجع زیست‌سنجشی واجد شرایط به‌وسیله یک نهاد مجاز (به عنوان مثال، هم ثبت‌شده مجاز و هم صاحب سامانه)، بدون مداخله حمله‌کننده؛
- اصلاح (شامل جایگزینی) یک مرجع زیست‌سنجشی از ثبت مجاز توسط یک حمله‌کننده

سامانه‌های زیست‌سنجشی بایستی حفاظت یکپارچگی داده‌های اثربخش را به کار گیرند. این موضوع می‌تواند از طریق راه‌کار واپایش دسترسی که از دسترسی‌های غیرمجاز به داده‌های زیست‌سنجشی جلوگیری می‌کند، و یا به‌وسیله بررسی‌های یکپارچگی که از فناوری‌های رمزگذاری استفاده می‌کند، درک شود. حفاظت یکپارچگی ممکن است نیاز به ترکیب شدن با سایر فناوری‌ها (مثل مهر زنی زمانی) داشته باشد تا در برابر دزدیده شدن داده‌های زیست‌سنجشی و تکرار حمله‌ها محافظت شود.

یادآوری ۱- فناوری‌های مختلف مثل کد اصالت‌سنجی پیام (MAC) یا امضای رقمی، می‌توانند برای تامین یکپارچگی داده استفاده شوند. برای اطلاعات بیشتر به پیوست ب-۲ رجوع شود.

یادآوری ۲- شرایط معین نیاز به هر دو مورد محرمانگی و یکپارچگی دارند. اگر هر دو حفاظت محرمانگی و یکپارچگی نیاز باشد، یک امکان این است که هم رمزگذاری و هم MAC یا امضای رقمی استفاده شود. امکان دیگر این است که رمزگذاری اصالت‌سنجی شده استفاده شود مثل استانداردسازی در استاندارد ISO /IEC 19772.

یادآوری ۳- وقتی یک کارت هوشمند برای ذخیره‌سازی و یا مقایسه مرجع زیست‌سنجشی استفاده می‌شود (بند ۸، الگوهای B، E،F، G و H)، توصیه می‌شود راه‌کار پیام‌رسانی امن مطابق با استاندارد ISO /IEC 7816-4 برای یکپارچگی و یا محرمانگی داده‌های زیست‌سنجشی استفاده شود.

۳-۱-۵ تجدیدپذیری و ابطال‌پذیری

نگرانی بزرگ امنیت و حریم خصوصی برای سامانه‌های زیست‌سنجشی به نقض مراجع زیست‌سنجشی مربوط می‌شود. تنوع تهدیدها می‌تواند یک مرجع زیست‌سنجشی را نقض کند. به عنوان مثال یک حمله‌کننده می‌تواند دسترسی غیرقانونی به یک نمودافزار حاوی مرجع زیست‌سنجشی داشته باشد یا ممکن است سعی کند به‌وسیله زیست‌سنجشی تقلبی یا کلاه‌برداری شده[1] از طریق پذیرش نادرست، دسترسی غیرقانونی کسب کند. در موارد نقض، برای اجتناب از حمله‌کننده‌های آینده (یا پیوسته) دسترسی غیرمجاز، ابطال‌پذیر الزامی است. متناوباً، ممکن است نقض امنیتی دادگان منجر به افشاگری غیرقانونی مراجع زیست‌سنجشی و سایر داده‌های شخصی شود. در مورد چنین نقض مراجع زیست‌سنجشی و برای همبستگی موضوع داده قانونی یا مرجع جدید زیست‌سنجشی نیاز سختی به ابطال مراجع زیست‌سنجشی وجود دارد. تذکر اینکه ابطال‌پذیری و تجدیدپذیری مرجع زیست‌سنجشی دلالت بر تجدید موضوع داده مشخصه‌های زیست‌سنجشی ندارد، توصیه می‌شود. تجدیدپذیری و ابطال‌پذیری فقط وسیله‌ای برای رفع مراجع زیست‌سنجشی نقض شده را تامین می‌کنند و برای مشخصه‌های زیست‌سنجشی نقض شده مناسب نیستند.

ممکن است یک مرجع زیست‌سنجشی در کنار نقض بنا به دلایل متنوعی نیاز به تغییر داشته باشد. به عنوان مثال ممکن است یک مرجع زیست‌سنجشی فقط برای دوره زمانی معینی (در حالت مشابه با گذرواژه‌ها) معتبر باشد. اگر مرجع زیست‌سنجشی در پایان دوره زمانی همچنان مورد نیاز باشد، ممکن است مرجع تجدید یا ابطال و جایگزین شود.

1 - Spoofed

۵-۲ تهدیدهای امنیتی و اقدام متقابل در سامانه‌های زیست‌سنجشی

۵-۲-۱ تهدیدها و اقدامات متقابل در برابر اجزای سامانه زیست‌سنجشی

تهدیدها در برابر اجزای سامانه زیست‌سنجشی در جدول ۱ خلاصه شده‌اند:

جدول ۱- تهدیدها و اقدامات متقابل سامانه‌های زیست‌سنجشی

	تهدیدها	اقدامات متقابل
اخذ داده	کلاه‌برداری حسگر اخذ/ بازپخش سیگنال‌ها از حسگر	- آشکارسازی زنده بودن - زیست‌سنجشی چند کیفیتی - چالش/پاسخ
پردازش سیگنال	دست‌کاری غیرمجاز داده در حین پردازش	- استفاده از الگوریتم قابل‌اعتماد
مقایسه	دست‌کاری امتیازات مقایسه	- کارخواه و/یا کارخواه امن - OCC قابل‌اعتماد
ذخیره‌سازی	نقض دادگان - افشاگری غیرمجاز IR/BR - جایگزینی غیرمجاز IR/BR - اصلاح غیرمجاز IR/BR - حذف غیرمجاز IR/BR	- مراجع زیست‌سنجشی ابطال‌پذیر و تجدیدپذیر - جداسازی داده - واپایش دسترسی به دادگان - علامت BR/RBR/IR - رمزگذاری BR/RBR/IR
تصمیم‌گیری	حمله بالا رفتن از تپه	- کانال امن - پنهان کردن امتیاز مقایسه از موضوع
	دست‌کاری آستانه	- واپایش دسترسی به تنظیمات آستانه - حفاظت از ارزش آستانه

یادآوری ۱- برای ارزشیابی امنیتی و گواهی اجزای پودمانی سامانه‌های زیست‌سنجشی و اطلاعات بیشتر به استاندارد ISO /IEC 19792 مراجعه شود.

یادآوری ۲- پیاده‌سازی اجزای مقایسه و تصمیم‌گیری در پودمان واحد گواهی شده، اقدام متقابل اثربخشی در برابر تهدیدهای دست‌کاری امتیاز مقایسه تشکیل می‌دهد. در اینجا اقدامات افزوده پنهان کردن امتیاز مقایسه از موضوع برای جلوگیری از حمله بالا رفتن از تپه[1] الزامی است.

یادآوری ۳- تهدید جابه‌جایی اجزا در تمام زیرسامانه‌ها کاربردپذیر است. اقدام متقابل اثربخش در برابر این تهدید، استفاده از فهرست واپایش شامل اجزای امضا شده رقمی است.

توضیح مختصر تهدیدها و اقدامات متقابل فوق‌الذکر در طبقه‌بندی زیر آورده شده است:

- کلاه‌برداری حسگر یعنی ارائه مشخصه‌های غیرزنده و مصنوعی است. یک اقدام متقابل در برابر

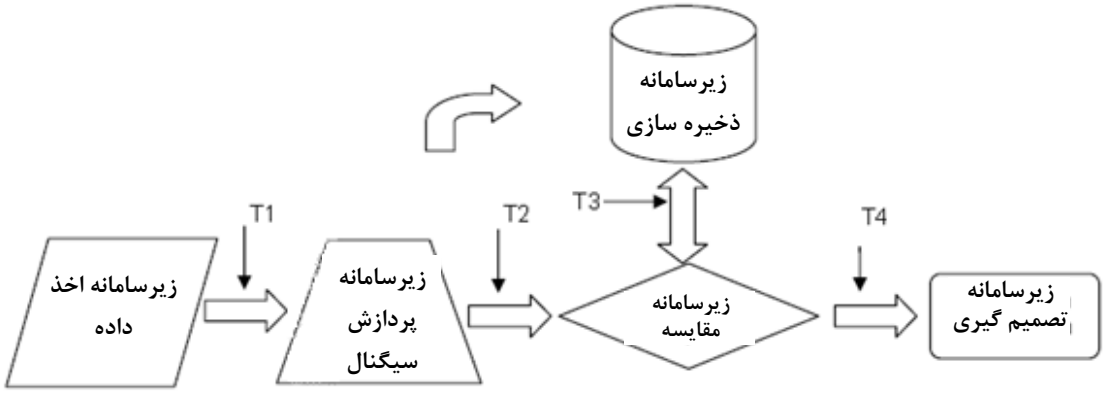
1 - Hill Climbing attack

کلاه‌برداری حسگر، آشکارسازی حیات بر اساس تشخیص فعالیت‌های کاراندام‌شناختی موضوع به عنوان نمودافزارای از زندگی یا آشکارسازی یا رد انواع مصنوع شناخته شده است.

- جایگزینی اجزا شامل جایگذاری اجزای سامانه زیست‌سنجشی (مثل زیرسامانه مقایسه یا تصمیم‌گیری) است، در نتیجه می‌توان آن را واپایش کرد و به خروجی مطلوب دست یافت.
- بالا رفتن از تپه یک اصلاح سامانه‌مند نمونه زیست‌سنجشی برای دست‌یابی به امتیاز بالاتر مقایسه به‌طور فزاینده است تا وقتی که آستانه تصمیم‌گیری برآورده شود.
- دست‌کاری آستانه، ارزش آستانه زیرسامانه تصمیم‌گیری را تغییر می‌دهد، در نتیجه سامانه زیست-سنجشی نمونه زیست‌سنجشی غیرقانونی را به سادگی می‌پذیرد.
- مراجع زیست‌سنجشی ابطال‌پذیر و تجدیدپذیر به‌وسیله مفهوم تنوع‌بخشی برای کاربردها، سازمان‌ها و شرکت‌های مختلف ایجاد می‌شوند اما در پیوند با موضوع مشابه هستند. موضوعات می‌توانند RBR های چندگانه داشته باشند.
- جداسازی داده مربوط به اقدامات متقابل امنیتی و جداسازی فیزیکی و منطقی اجزای داده‌های اشخاص می‌شود (مانند بخشی از نمودافزار و بخشی از دادگان، همچنین به بند ۷-۲ مراجعه شود). جداسازی داده می‌تواند برای اجزای داده مثل IR، BR، PI، AD به کار گرفته شود.

۵-۲-۲ تهدیدها و اقدامات متقابل در حین انتقال اطلاعات زیست‌سنجشی

کانال‌های ارتباطی بین اجزای متنوع سامانه زیست‌سنجشی می‌تواند نقض شود و امنیت کل سامانه را به خطر اندازد. این مخاطره مخصوصاً به معماری‌ها توزیع شده است. دقت انتقال داده در شکل ۴ نشان داده و در جدول-۲ مختصر شده است. در جدول-۲ اگر یک شبکه بین زیرسامانه‌های مقایسه و تصمیم‌گیری مداخله کند، تهدید و اقدامات متقابل آن ها برای T1، T2، T3 و همچنین T4 کاربردپذیر است.



شکل ۴- تهدیدها در یک سامانه زیست‌سنجشی

جدول ۲- تهدیدها و اقدامات متقابل در حین انتقال

	داده	تهدید	اقدام متقابل
اخذ داده- پردازش سیگنال (T1) **پردازش سیگنال- مقایسه (T2)**	نمونه و ویژگی زیست‌سنجشی	استراق سمع کردن	- کانال امن / رمزگذاری شده
		بازپخش	- چالش/پاسخ
		آزمون و خطا	- وقفه
ذخیره‌سازی- مقایسه (T3)	مرجع زیست‌سنجشی	استراق سمع کردن	- کانال امن / رمزگذاری شده
		بازپخش	- چالش/پاسخ
		مرد میانی[1]	- کانال امن / رمزگذاری شده - بررسی یکپارچگی داده زیست‌سنجشی با امضای رقمی یا MAC
		بالا رفتن از تپه	- امتیازات درشت - کانال امن
مقایسه- تصمیم‌گیری (T4)	امتیاز مقایسه	دست‌کاری امتیاز مقایسه	- کانال امن

یادآوری- پیاده‌سازی اجزای مقایسه و تصمیم‌گیری در یک پودمان گواهی شده، اقدام متقابل اثربخشی در برابر تهدید دست‌کاری امتیاز مقایسه تشکیل می‌دهد.

توضیح مختصر در مورد تهدیدهای فوق‌الذکر در طبقه‌بندی زیر آورده شده است:

- استراق سمع کردن، قطع کردن اطلاعات حساس در حین انتقال بین اجزای سامانه زیست‌سنجشی است.
- انسان در میانه حملات، حملاتی است که در آن حمله‌کننده می‌تواند داده‌های زیست‌شناسی مرتبط بین دو قسمت را بخواند، وارد کند و یا اصلاح نماید، بدون اینکه هرکدام از قسمت‌ها بدانند که پیوند تاسیس شده تحت نقض است.

فهرست اقدامات متقابل در جدول ۲ جامع نیستند. توصیه می‌شود یک تحلیل مخاطره برای شناسایی تهدیدها در متن برنامه کاربردی اجرا شود. توصیه می‌شود اقدام متقابل مناسب در محل‌هایی که می‌تواند شامل اقدامات متقابل دارای روش اجرایی و فنی باشد، برقرار شود. برای توضیحات بیشتر در مورد جنبه‌های مدیریتی حفاظت از سامانه‌های زیست‌سنجشی به استانداردهای ISO 19092:2008, LTV-TX 1086 و

1 - Man in the middle

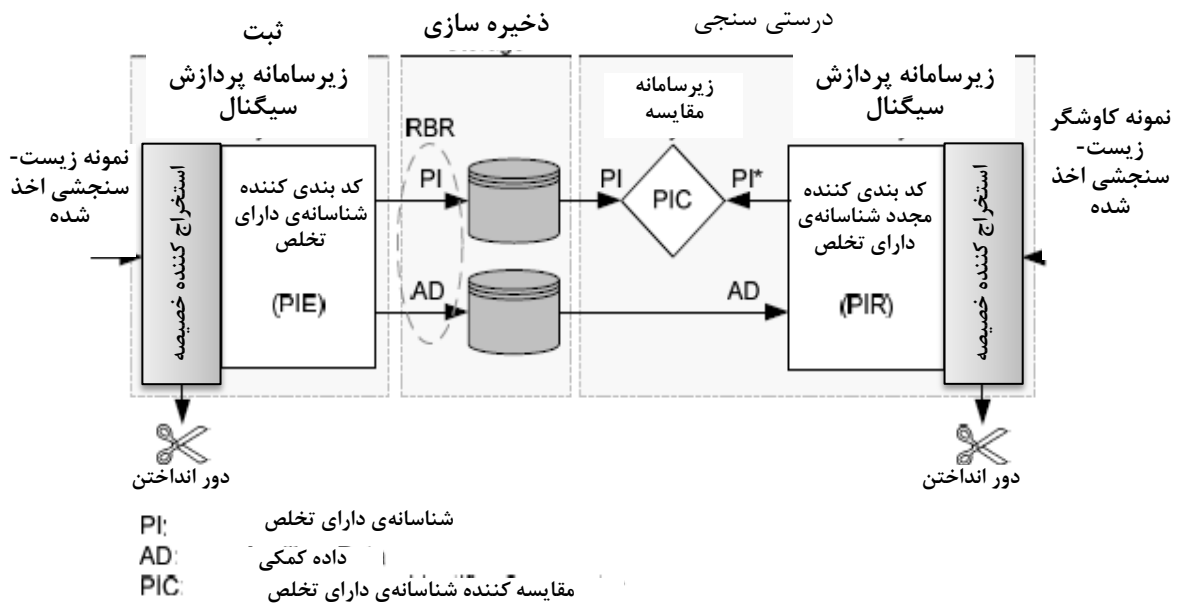
ISO/IEC 19792 مراجعه شود.

۵-۲-۳ مراجع زیست‌سنجشی تجدیدپذیر به عنوان فناوری اقدام متقابل

قابلیت تجدیدپذیری مرجع زیست‌سنجشی یک اقدام متقابل در برابر تهدیدهای ذخیره‌سازی و انتقال است. به منظور مجاز کردن ابطال‌پذیری یا تجدیدپذیری مرجع زیست‌سنجشی، توصیه می‌شود فرایند ایجاد مرجع زیست‌سنجشی فرایند تنوع‌بخشی را پشتیبانی کند. تنوع‌بخشی شامل تولید مراجع چندگانه مستقل از مشخصه‌های زیست‌سنجشی مشابه است که می‌تواند برای تجدید یک مرجع زیست‌سنجشی یا تامین مراجع مستقل در میان کاربردهای مختلف استفاده شود. توصیه می‌شود فرایند تنوع‌بخشی تغییرناپذیر باشد. توصیه می‌شود مراجع زیست‌سنجشی انتقال داده شده به‌طور منحصر به فرد قابل پیوند نباشند.

به منظور تسهیل سازی واژه‌نامه رایج برای پیاده‌سازی مراجع زیست‌سنجشی تجدیدپذیر (RBR_S) از طریق یک فرایند تنوع‌بخشی و برای مطرح کردن جنبه‌های معماری گونه مراجع زیست‌سنجشی تجدیدپذیر و فرایند تنوع‌بخشی در یک حالت خنثی از فناوری، مفهوم شناسانه‌ی دارای تخلص در این استاندارد استفاده‌شده است. در رویکرد شرح داده شده در این استاندارد، مراجع زیست‌سنجشی تجدیدپذیر شامل دو عنصر داده هستند: یک شناسانه‌ی دارای تخلص (PI) و داده کمکی متناظر (AD). هر دو عنصر داده در طی ثبت تولیدشده‌اند و باید ذخیره شوند زیرا هر دو عنصر در حین فرایند شناسایی یا درستی سنجی مورد نیاز هستند.

یک مرور کلی از جنبه‌های معماری گونه مراجع زیست‌سنجشی تجدیدپذیر در شکل ۵ تامین شده است. پیکان در شکل جریان اطلاعات را ارائه می‌دهد. در حین ثبت، یک مرحله استخراج خصیصه داده خصیصه زیست‌سنجشی از نمونه زیست‌سنجشی اخذشده تولید می‌کند. متعاقباً یک کدبند شناسانه‌ی دارای تخلص (PIE) مرجع زیست‌سنجشی تجدیدپذیر تولید می‌کند که شامل شناسانه‌ی دارای تخلص (PI) و داده کمکی (AD) است. وقتی RBR تولید شد، نمونه زیست‌سنجشی اخذشده و خصیصه‌های استخراج‌شده می‌توانند به‌طور امن مرتب شوند. RBR در یک کارت متوسط ذخیره‌سازی مناسب (مثل کارت هوشمند یا دادگان الکترونیکی) ذخیره می‌شود. ممکن است PI و AD به‌طور فیزیکی یا منطقی از هم جدا شده باشند. در حین درستی سنجی، یک مرحله استخراج خصیصه نمونه زیست‌سنجشی کاوشگر را پردازش می‌کند. متعاقباً یک کدبند شناسانه‌ی دارای تخلص (PIR) یک شناسانه‌ی دارای تخلص (PI^*) بر اساس داده کمی و خصیصه‌های استخراج‌شده و تامین شده می‌سازد. متعاقبا زیرسامانه مقایسه PI تولیدشده در حین ثبت و PI^* را مقایسه می‌کند و شباهت امتیاز را که شباهت بین PI و PI^* را ارائه می‌دهد، بازمی‌گرداند. مرور کلی گسترده‌تر از ایجاد شناسانه‌ی دارای تخلص و فرایند درستی سنجی و همچنین چرخه زیستی آن در پیوست پ تامین شده است.



شکل ۵- معماری برای مراجع زیست‌سنجشی تجدیدپذیر

۵-۳ امنیت داده‌های گزارش‌شده شامل اطلاعات زیست‌سنجشی

۵-۳-۱ امنیت برای اطلاعات زیست‌سنجشی پردازش‌شده در یک دادگان

یک تسلسل منطقی از مرجع شناسه (IR) با یک مرجع زیست‌سنجشی (BR) برای اجرای عملکردهای اصالت‌سنجی زیست‌سنجشی الزامی است و در شکل ۱ نشان داده شده است. تعداد زیادی فرانامه کاربردپذیر وجود دارد که می‌تواند برای شرح این پیوند استفاده شود و بر اساس داده‌های گزارش‌شده (مثل مرجع شناسه، مرجع زیست‌سنجشی و غیره) ذخیره شود. این فرانامه‌ها ترکیبات عناصر داده را نشان می‌دهند و همچنین همبستگی ویژگی‌های امنیتی را مطرح می‌کنند. فهرست زیر این فرانامه‌ها را شرح می‌دهد:

فرانامه ۱: مرجع شناسه (IR) و مرجع زیست‌سنجشی (BR) خام ذخیره‌شده‌اند. نه محرمانگی و نه یکپارچگی برای IR و BR تامین نشده است. تجدیدپذیری و ابطال‌پذیری تامین نشده‌اند.

فرانامه ۲: مرجع شناسه (IR) خام BR رمزگذاری‌شده ذخیره‌شده‌اند. نه محرمانگی و نه یکپارچگی برای IR تامین نشده است. محرمانگی برای BR تامین شده است. ممکن است یک شکل ضعیف از یکپارچگی برای BR تامین شده باشد که وابسته به حالت عملکرد رمزگذاری است. تجدیدپذیری و ابطال‌پذیری تامین نشده‌اند.

فرانامه ۳: مرجع شناسه (IR) خام و BR اصالت‌سنجی‌شده ذخیره‌شده‌اند. فقط یکپارچگی BR تامین شده است.

فرانامه ۴: مرجع شناسه (IR) خام و قالب اصالت‌سنجی‌شده و رمزگذاری‌شده‌ی BR ذخیره‌شده‌اند. هم محرمانگی و هم یکپارچگی برای BR تامین شده است.

فرانامه ۵: مرجع شناسه (IR) رمزگذاری‌شده و BR خام ذخیره‌شده‌اند. محرمانگی برای IR تامین شده است. ممکن است یک شکل ضعیف از یکپارچگی برای IR تامین شده باشد که بستگی به حالت عملکرد رمزگذاری دارد.

فرانامه ۶: مرجع شناسه (IR) اصالت‌سنجی‌شده و BR خام ذخیره‌شده‌اند. فقط یکپارچگی IR تامین شده است.

فرانامه ۷: شکل اصالت‌سنجی‌شده و رمزگذاری IR و BR خام ذخیره‌شده‌اند. محرمانگی و یکپارچگی فقط برای IR تامین شده‌اند.

فرانامه ۸: مرجع شناسه (IR) و BR خام رمزگذاری و ذخیره‌شده‌اند. محرمانگی هم برای IR و هم برای BR تامین شده است. ممکن است یک شکل ضعیف از یکپارچگی هم برای IR و هم برای BRتامین شده باشد که بستگی به حالت عملکرد رمزگذاری دارد.

فرانامه ۹: مرجع شناسه (IR) و BR خام اصالت‌سنجی‌شده و ذخیره‌شده‌اند. یکپارچگی هم برای IR و هم برای BR تامین شده است.

فرانامه ۱۰: شکل اصالت‌سنجی‌شده و رمزگذاری شده IR و BR ذخیره‌شده‌اند. محرمانگی و یکپارچگی هم برای IR و هم برای BR تامین شده است.

فرانامه ۱۱: مرجع شناسه (IR) خام و BR اصالت‌سنجی‌شده رمزگذاری و سپس ذخیره‌شده‌اند. محرمانگی هم برای IR و هم برای BR تامین شده است. یکپارچگی برای BR تامین شده است. ممکن است یک شکل ضعیف از یکپارچگی بر اساس حالت عملکرد رمزگذاری تامین شده باشد.

فرانامه ۱۲: مرجع شناسه (IR) خام و BR رمزگذاری شده اصالت‌سنجی‌شده و سپس ذخیره‌شده‌اند. یکپارچگی هم برای IR و هم BR تامین شده است. محرمانگی فقط برای BR تامین شده است.

فرانامه ۱۳: مرجع شناسه (IR) اصالت‌سنجی‌شده و BR خام رمزگذاری و سپس ذخیره‌شده‌اند. محرمانگی هم برای IR و هم BR تامین شده است. یکپارچگی برای IR تامین شده است. ممکن است یک شکل ضعیف از یکپارچگی بر اساس عملکرد الگوریتم رمزگذاری اصولی برای BR تامین شده باشد.

فرانامه ۱۴: مرجع شناسه (IR) رمزگذاری‌شده و BR خام، اصالت‌سنجی شده و سپس ذخیره شده‌اند. یکپارچگی هم برای IRو هم BR تامین شده است. محرمانگی فقط برای IR تامین شده است.

فرانامه ۱۵: مرجع شناسه (IR) خام و BR متنوع‌شده، ذخیره‌شده‌اند. تجدیدپذیری و ابطال‌پذیری و همچنین محرمانگی و یکپارچگی محدود برای BR تامین شده‌اند.

فرانامه ۱۶: مرجع شناسه (IR) خام و BR متنوع‌شده، اصالت‌سنجی شده و سپس ذخیره شده‌اند. یکپارچگی هم برای IR و هم BR تامین شده است. تجدیدپذیری و ابطال‌پذیری برای BR تامین شده‌اند.

فرانامه ۱۷: شکل اصالت‌سنجی‌شده و رمزگذاری‌شده IR و BR متنوع‌شده، ذخیره‌شده‌اند. یکپارچگی و محرمانگی هم برای IR و هم برای BR تامین شده است. تجدیدپذیری و ابطال‌پذیری برای BR تامین شده‌اند.

فرانامه ۱۸: مرجع شناسه (IR) خام و BR متنوع‌شده رمزگذاری و سپس ذخیره‌شده‌اند. محرمانگی هم برای IR و هم BR تامین شده است. ممکن است یک شکل ضعیف از یکپارچگی بر اساس حالت عملکرد برای IR و BR تامین شده باشد. تجدیدپذیری و ابطال‌پذیری برای BR تامین شده‌اند.

فرانامه ۱۹: مرجع شناسه (IR) خام و BR رمزگذاری و متنوع‌شده[1] اصالت‌سنجی‌شده و سپس ذخیره‌شده‌اند. یکپارچگی هم برای IR و هم BR تامین شده است. محرمانگی، تجدیدپذیری و ابطال‌پذیری برای BR تأمین شده‌اند.

فرانامه‌ها شرح داده شده مربوط به ملاحظات امنیتی در جدول ۳ خلاصه شده‌اند.

جدول ۳- محرمانگی، یکپارچگی و تجدیدپذیری برای داده‌های گزارش و ذخیره‌شده در یک دادگان

(Enc'd: رمزگذاری شده، Aut'd: اصالت‌سنجی‌شده و رمزگذاری شده، Div'd: متنوع‌شده ، O: الزامات، Δ: الزامات ضعیف)

فرانامه	الزامات امنیتی					اقدامات متقابل
	تجدیدپذیری	یکپارچگی		محرمانگی		
	BR	BR	IR	BR	IR	
۲		Δ		O		Raw IR and Enc'd BR
۳		O				Raw IR and Aut'd BR
۴		O		O		Raw IR and AuE'd BR
۵			Δ		O	Enc'd IR and Raw BR
۶			O			Aut'd IR and Raw BR
۷			O		O	AuE'd IR and Raw BR
۸		Δ	Δ	O	O	Enc'd(IR and BR)

1 - Diversified

فرانامه	الزامات امنیتی					اقدامات متقابل
	تجدیدپذیری	یکپارچگی		محرمانگی		
	BR	BR	IR	BR	IR	
۹		O	O			Aut'd(IR and BR)
۱۰		O	O	O	O	AuE'd(IR and BR)
۱۱		O	Δ	O	O	Enc'd(IR and Aut'd BR)
۱۲		O	O	O		Aut'd(IR and Enc'd BR)
۱۳		Δ	O	O	O	Enc'd(Aut'd IR and BR)
۱۴		O	O		O	Aut'd(Enc'd IR and BR)
۱۵	O					Raw IR and Div'd BR
۱۶	O	O	O	Δ		Aut'd(IR and Div'd BR)
۱۷	O	O	O	O	O	AuE'd(IR and Div'd BR)
۱۸	O	Δ	Δ	O	O	Enc'd(IR and Div'd BR)
۱۹	O	O	O	O		Aut'd(IR and Enc'd, Div'd BR)

استاندارد ISO/IEC 19785 چارچوب نسبت تبادل زیست‌سنجشی معمولی (CBEFF) را برای ارتقای قابلیت همکاری سامانه‌ها و عملکردها بر اساس زیست‌سنجشی به‌وسیله معین کردن ساختار استاندارد برای گزارش‌های اطلاعات زیست‌سنجشی (BIRS) معین می‌کند. در استاندارد ISO /IEC 19785-4، نسبت‌های بلوک امنیتی (SB) به منظور حفظ یکپارچگی (BIRS) و به منظور رمزگذاری / رمزگذاری نکردن داده‌های زیست‌سنجشی در BIR معین شده‌اند.

۲-۳-۵ امنیت برای اطلاعات زیست‌سنجشی که در بانک‌های اطلاعات جداگانه پردازش می‌شود

وقتی IR، BR، RBR ذخیره می‌شوند، اگر حریم خصوصی الزامی است، پیشنهاد می‌شود آن ها به‌طور جداگانه ذخیره گردند زیرا افشاگری هر دو مورد منجر به نقض جدی حریم خصوصی می‌شود. حتی اگر IR و BR به محدوده‌های ذخیره‌سازی متفاوتی جدا شوند، در صورت واپایش شدن آن ها توسط عملگر مشابه، حفاظت اثربخش نخواهد بود. برای اثربخش کردن جداسازی، توصیه می‌شود آن ها توسط عملگرهای متفاوت با کلیدهای رمزگذاری آن‌ها واپایش شوند تا از محتوی DB خود حفاظت کنند. هرگاه IR و BR جدا شوند، توصیه می‌شود وسیله‌ای برای پیوند آن ها وجود داشته باشد. این هدف به‌وسیله شناسانه عام CI به دست

می‌آید. بحث مشابهی برای ذخیره‌سازی RBRS در شکل PI و AD مطرح است. جداسازی فیزیکی و یا منطقی PI و AD مخاطره‌های حریم خصوصی و امنیت را کاهش می‌دهد. جداسازی فیزیکی مطلوب است. اگر نمودافزارها در یک الگو بر اساس ذخیره‌سازی توزیع شده به کار گرفته شوند، توصیه می‌شود AD روی نمودافزار و PI روی کارخواه[1] یا کارساز[2] ذخیره شوند. اگر DB های جدا شده و CI معمولی به کار گرفته شوند، توصیه می‌شود دادگان توسط عملگرهای جدا با کلیدهای رمزگذاری متفاوت واپایش شوند.

در جدول ۴ فرانامه‌ها به‌کارگیری دادگان جداگانه نشان داده شده است. الزامات امنیتی محرمانگی، یکپارچگی، تجدیدپذیری و ابطال‌پذیری به‌طور مشابه باقی می‌ماند. به هر حال تاثیر نقض حریم خصوصی کوچک‌تر می‌شود حتی اگر یکی از IR ها یا BR ها افشا شوند. اگر یک DB نقض شود و محتوی آن به‌طور غیرقانونی اصلاح گردد، توصیه می‌شود عملگرهای دو BD قادر باشند آن را آشکار کنند. به‌طور مشابه، در حین استفاده از DB ها، اگر عملگر قانونی آن محتوی آن را با کلید صحیح اصلاح کند، توصیه می‌شود سایر DB ها قادر به آشکار کردن آن اصطلاحات باشند. برای این موارد، پیوندهای امنیتی بیشتر الزامی است. پیوست الف مثال‌هایی از پیاده‌سازی شناسانه عام (CI) را تامین می‌کند.

جدول ۴- محرمانگی، یکپارچگی و تجدیدپذیری برای گزارش‌های داده ذخیره‌شده در دادگان جداگانه

(Enc'd: رمزگذاری شده، Aut'd: اصالت‌سنجی‌شده و رمزگذاری شده، Div'd: متنوع‌شده، O: الزامات، Δ: الزامات ضعیف)

اقدامات متقابل برای BR	اقدامات متقابل برای IR	الزامات امنیتی				
		محرمانگی		یکپارچگی		تجدیدپذیری
		IR	BR	IR	BR	BR
CI, Enc'd BR	CI, Raw IR		**O**		**Δ**	
CI, Aut'd BR	CI, Raw IR				**O**	
CI, AuE'd BR	CI, Raw IR		**O**		**O**	
CI, Raw BR	CI, Enc'd IR	**O**		**Δ**		
CI, Raw BR	CI, Aut'd IR			**O**		
CI, Raw BR	CI, AuE'd IR	**O**		**O**		
CI, Enc'd BR	CI, Enc'd IR	**O**	**O**	**Δ**	**Δ**	
CI, Aut'd BR	CI, Aut'd IR			**O**	**O**	

1 - Client

2 - Server

اقدامات متقابل برای BR	اقدامات متقابل برای IR	الزامات امنیتی				
		محرمانگی		یکپارچگی		تجدیدپذیری
		IR	BR	IR	BR	BR
CI, AuE'd BR	CI, AuE'd IR	O	O	O	O	
CI, AuE'd BR	CI, Enc'd IR	O	O	Δ	O	
CI, AuE'd BR	CI, Aut'd IR		O	O	O	
CI, Enc'd BR	CI, AuE'd IR	O	O	O	Δ	
CI, Aut'd BR	CI, AuE'd IR	O		O	O	
CI, AD	CI, PI, IR					O
CI, Aut'd AD	CI, Aut'd PI, Aut'd IR		Δ	O	O	O
CI, AuE'd AD	CI, AuE'd(PI and IR)	O	O	O	O	O
CI, Enc'd AD	CI, Enc'd(PI and IR)	O	O	Δ	Δ	O
CI, Aut'd(Enc'd AD)	CI, Aut'd(Enc'd PI and IR)	O	O	O	O	O

۶ مدیریت حریم خصوصی اطلاعات زیست‌سنجشی

۶-۱ تهدیدهای حریم خصوصی اطلاعات زیست‌سنجشی

از آنجایی که داده‌های زیست‌سنجشی، PII هستند، توصیه می‌شود استاندارد ISO /IEC 29100، که سامانه نشانی‌دهی چارچوب کلی حریم خصوصی برای معین کردن موارد در سطح بالا می‌باشند، به کار گرفته شود. این یک چارچوب کلی است که جنبه‌های سازمانی، فنی، اجرایی و تنظیمی حریم خصوصی برای سامانه‌های فناوری اطلاعات را نشان می‌دهد.

سامانه‌ها اطلاعات شخصی را پردازش و ذخیره می‌کنند. استفاده از داده‌های زیست‌سنجشی تهدیدهای متعددی برای حریم خصوصی که نشانی می‌شود را شامل می‌گردد:

- ممکن است از داده‌های زیست‌سنجشی برای اهدافی غیر از نامزدهای اصلی و رضایت داده شده به‌وسیله موضوع داده سوء استفاده شود.

- ممکن است مراجع زیست‌سنجشی اجازه بازیابی یا تحلیل ویژگی‌های موضوع داده که برای شناسایی یا درستی سنجی زیست‌سنجشی الزامی نیستند بدهد، مثل حالت سلامتی یا اطلاعات پزشکی استنتاجی و پس‌زمینه نژادی موضوع داده.
- ممکن است از مراجع زیست‌سنجشی برای انقیاد موضوعات در بین کاربردهای متفاوت در یک دادگان مشابه یا در بین دادگان متفاوت استفاده شود. حریم خصوصی مربوط به مرجع زیست-سنجشی ذخیره‌شده پیوند ناپذیر است.

توضیحات بیشتر یا ملاحظات اجتماعی و قضایی برای کاربردهای تجاری زیست‌سنجشی در استاندارد ISO/IEC TR24714-1 آمده است.

۶-۲ الزامات و راهنمایی‌های حریم خصوصی اطلاعات زیست‌سنجشی

۶-۲-۱ بازگشت‌ناپذیری

برای جلوگیری از استفاده داده زیست‌سنجشی برای هر هدف به‌جز نامزدهای اصلی، داده زیست‌سنجشی باید توسط انتقال بازگشت‌ناپذیر قبل از ذخیره‌سازی پردازش شود. ممکن است بازگشت‌ناپذیری با استفاده از راهکارهای زیر که می‌توانند ترکیبی باشند، به دست آید:

- الگوریتم‌های استخراج خصیصه اغلب یک شکل از بازگشت‌ناپذیری را به‌وسیله اختصار و حذف زوائد داده‌ها تامین می‌کنند و دشواری استفاده از خصیصه‌های استخراج‌شده را برای استخراج داده‌های پزشکی یا نژادی افزایش می‌دهند.
- رمزگذاری فقط از یک کلید شناخته شده به‌وسیله عملگر سامانه استفاده می‌کند و یا موضوع داده، دسترسی‌های غیرقانونی به داده زیست‌سنجشی را محدود می‌سازد.

شناسانه‌های دارای تخلص وسیله‌ای برای محدود کردن دسترسی به مشخصه‌های زیست‌سنجشی داده موضوع را به‌وسیله انتقال‌های بازگشت‌ناپذیر تامین می‌کنند. یک مرور کلی از انتقال‌ها که شناسانه‌های دارای تخلص تولید می‌کند در پیوست ت و جدول ت-۱ تامین شده است.

۶-۲-۲ پیوند ناپذیری

توصیه می‌شود مراجع زیست‌سنجشی ذخیره‌شده در بین کاربردها یا دادگان پیوندپذیر نباشند. پیوند ناپذیری می‌تواند با استفاده از راهکارهای متفاوت که ترکیب می‌شوند تامین شود.

- اگر مراجع زیست‌سنجشی با متن اصلی پیوندپذیر باشند، رمزگذاری کردن مراجع زیست‌سنجشی که راهکارها یا کلیدهای (مخفی) متفاوتی در میان کاربردها به کار می‌گیرند، از پیوند موضوعات داده جلوگیری می‌کند، در نتیجه کلیدهای مخفی برای امتناع از تبانی به‌طور مناسبی مدیریت می‌شوند.
- شناسانه‌های دارای تخلص پیوند ناپذیر و مستقل که از طریق فرایند تنوع‌بخشی ایجاد می‌شوند، از

پیوند موضوعات داده جلوگیری می‌کنند.

- جداسازی فیزیکی یا منطقی IR و BRیا PI و AD در مورد RBR ها از دسترسی به گزارش‌های کامل داده جلوگیری می‌کنند.
- استفاده از کیفیت‌های زیست‌سنجشی متفاوت، الگوریتم‌های استخراج خصیصه ناسازگار، یا تبادل اشکالی داده زیست‌سنجشی از طریق کاربردها از پیوند موضوعات داده جلوگیری می‌کند.

یادآوری- ممکن است استفاده از کیفیت‌های متفاوت زیست‌سنجشی، الگوریتم‌های استخراج خصیصه ناسازگار یا تبادل اشکال داده چالش‌های مربوط به قابلیت همکاری سامانه را مطرح کند.

۶-۲-۳ محرمانگی

برای محافظت از مراجع زیست‌سنجشی در برابر دسترسی به‌وسیله یک هستار غیرقانونی که منجر به مخاطره حریم خصوصی می‌شود، مراجع زیست‌سنجشی باید به‌طور محرمانگ نگهداری شوند. راهکارهای زیر می‌تواند برای تامین محرمانگی به کار رود:

- جداسازی داده به‌وسیله ذخیره کردن (بخشی از) مراجع زیست‌سنجشی در یک نمودافزار شخصی یا کارت به جای استفاده از دادگان متمرکز یک اقدام متقابل برای کاستن مخاطره‌های حریم خصوصی است که از نقض امنیتی دادگان متمرکز منجر می‌شود (به عنوان مثال هرگاه یک متخاصم دسترسی غیرمجازی به دادگان متمرکز به دست آورد و محتوی آن را منتشر کند).
- رمزگذاری کردن مراجع زیست‌سنجشی با استفاده از فقط یک کلید شناخته شده برای عملگر سامانه مدیریت شناسه و/ یا موضوع داده

یادآوری- استفاده از نمودافزار برای ذخیره داده زیست‌سنجشی ضمانت محرمانگی نیست مگر اینکه داده به‌طور فیزیکی و منطقی از افشاگری حفاظت شود.

۶-۳ الزامات خط‌مشی و مقررات تنظیمی[1]

همانند PII، جمع‌آوری، انتقال، استفاده، ذخیره‌سازی و انهدام مرجع زیست‌سنجشی به‌وسیله قوانین[2] و مقررات تنظیمی متنوع شامل حریم خصوصی و حفاظت داده واپایش می‌شوند. تمام گسترش‌های فناوری زیست‌سنجشی باید در تطابق با تمام قوانین و تنظیمات کاربردپذیر پیاده‌سازی شود.

1 - Regulations
2 - Laws

۶-۴ مدیریت حریم خصوصی چرخه زندگی اطلاعات زیست‌سنجشی

۶-۴-۱ جمع‌آوری[1]

سازمان ها باید رضایت موضوع را قبل از جمع‌آوری اطلاعات زیست‌سنجشی به دست آورند مگر اینکه قوانین و تنظیمات کاربردپذیر طور دیگری تعریف شوند. وقتی رضایت موضوع به دست آمد، توصیه می‌شود سازمان آگاهی کاملی از موارد زیر در اختیار موضوع قرار دهد (یادآوری می‌شود فهرست زیر جامع نیست):

- انواع و مقدار اطلاعات زیست‌سنجشی که اخذشده است.
- اطلاعات راجع به روش‌های اجرایی جایگزین در مواردی که موضوع داده یا نمی‌خواهد و یا نمی‌تواند در فهرست وارد شود.
- هدف جمع‌آوری و دوره زمانی نگهداری اطلاعات زیست‌سنجشی
- یک توضیح از چگونگی پردازش شدن اطلاعات زیست‌سنجشی اخذشده در سامانه زیست‌سنجشی و
- اطلاعات در مورد شخصی که مسئول مدیریت اطلاعات زیست‌سنجشی است که شامل نام، سازمان، منصب، اطلاعات تماس و غیره اوست.

جمع‌آوری غیرمجاز اطلاعات زیست‌سنجشی بدون مجوز تنظیمی تاثیر قدرتمندی در حریم خصوصی اطلاعات زیست‌سنجشی اشخاص دارد. با اینکه ممکن است یک سازمان رضایت موضوع را برای ایجاد مراجع زیست‌سنجشی داشته باشد، توصیه می‌شود همچنان فقط کمترین مقدار اطلاعات زیست‌سنجشی ضروری برای برآوردن اهداف مورد نظر استخراج شود. این امر باعث کاهش تاثیرِ نقض می‌شود.

۶-۴-۲ انتقال (افشای اطلاعات برای شخص سوم)

در هنگام انتقال اطلاعات زیست‌سنجشی به سازمان‌های دیگر، هر طرف درگیر در پردازش اطلاعات زیست-سنجشی باید موافق محدود بودن به‌وسیله قرارداد یا التزام حفاظت اطلاعات باشد. انتقال اطلاعات زیست-سنجشی باید فقط با رضایت موضوع اتفاق افتد، مگر اینکه رضایت به‌وسیله تدارک خدمات مورد درخواست موضوع یا قانون به دست آید.

قبل از رضایت‌مندی موضوع، توصیه می‌شود سازمان موارد زیر را تامین کند (یادآوری می‌شود فهرست جامع نیست):

- اطلاعات مناسب در مورد شخص سوم که اطلاعات زیست‌سنجشی به آن انتقال داده شده است.
- رضایت و مقدار اطلاعات زیست‌سنجشی منتقل شده و
- هدف انتقال و دوره زمانی نگهداری اطلاعات زیست‌سنجشی.

1 - Collection

از نقطه نظر موضوع، انتقال اطلاعات زیست‌سنجشی به شخص سوم اساساً مشابه ارائه مستقیم اطلاعات زیست‌سنجشی به شخص سوم است. بنابراین رضایت موضوع الزامی است مگر اینکه توسط قانون مجاز باشد. انتقال‌های از میان مرز مخصوصاً در عملکرد سامانه‌های زیست‌سنجشی شامل واپایش مرز و گذرنامه‌های الکترونیکی و غیره رایج است. به این منظور، مهم است که مراقبت بیشتری با رعایت حریم خصوصی اطلاعات زیست‌سنجشی منتقل شده که ممکن است توسط شخص سوم پردازش شود، انجام گیرد.

۶-۴-۳ استفاده

استفاده مربوط به دسترسی، پردازش یا اصلاحات اطلاعات زیست‌سنجشی در یک سازمان است. اطلاعات زیست‌سنجشی باید فقط با رضایت موضوع استفاده شود مگر اینکه توسط قانون معین شده باشد. اگر سازمان نخواهد از اطلاعات زیست‌سنجشی جمع‌آوری‌شده برای اهدافی به‌جز آن‌هایی که توسط موضوع معین شده‌اند استفاده کند، باید به رضایت موضوع دسترسی داشته باشد و توضیح کاملی از هدف اضافه شده برای استفاده و دوره زمانی نگهداری اطلاعات زیست‌سنجشی بیان کند. باید از ظهور عملکرد یا استفاده گسترده از اطلاعات زیست‌سنجشی مثل معین کردن سلامت یا میراث ژنتیکی موضوع پرهیز شود.

۶-۴-۴ ذخیره‌سازی

اطلاعات زیست‌سنجشی در بیشتر اوقات در زیرسامانه‌های ذخیره‌سازی داده ذخیره می‌شوند. همان‌گونه که در شکل ۱ توضیح داده شد که ممکن است توزیع شود. به منظور برآوردن الزامات حریم خصوصی ممکن است ذخیره اطلاعات با این چنین روش‌ها که می‌تواند به PII حساس شناسایی شوند، ضروری باشد. توصیه می‌شود سازمان ها اطلاعات زیست‌سنجشی جمع‌آوری‌شده را به‌صورت فیزیکی یا منطقی از سایر PII های موضوع جدا نگهدارند تا تاثیرات روی حریم خصوصی موضوع از اطلاعات ترکیبی نقض شده را کاهش دهند. اندازه‌های حفاظت کافی که در بند ۶ توضیح داده شد، برای اطمینان از محرمانگی و یکپارچگی اطلاعات زیست‌سنجشی و همچنین IR مربوط به آن ضروری است. برای پیگردی توزیع غیرقانونی و سوء استفاده از نمونه‌های زیست‌سنجشی، طرح‌واره‌های ته‌نقش‌گذار زیست‌سنجشی که در پیوست ث توضیح داده شده‌اند، می‌توانند در تطابق باشند مگر اینکه ضرورتاً از ذخیره‌سازی نمونه‌های زیست‌سنجشی خواسته شده که می‌توانند در طبقه‌بندی به عنوان PII قرارگیرند جلوگیری شود.

۶-۴-۵ بایگانی و پشتیبانی داده

بایگانی فرایند ذخیره‌سازی اطلاعات زیست‌سنجشی برای مدت طولانی یا نگهداری دائمی است. هرگاه سازمان اطلاعات زیست‌سنجشی را با رضایت موضوع جمع‌آوری کند، ممکن است رضایت حاوی یک تاریخ انقضاء برای معین کردن دوره زمانی ذخیره‌سازی اطلاعات زیست‌سنجشی اخذشده باشد. نگهداری اطلاعات زیست‌سنجشی بایگانی شده بیشتر از تاریخ انقضا می‌تواند شرایط رضایت را نقض و مخاطره نقض حریم خصوصی را ایجاد کند. همچنین محدودیت‌های دسترسی به اطلاعات زیست‌سنجشی بایگانی شده باید آن را برای اطلاعات زیست‌سنجشی عملیاتی هم‌ارز بازتاب دهد.

پشتیبانی داده، اگرچه بنا به دلایل مختلف بیشتر از بایگانی استفاده می‌شود، اگر به‌طور مناسب حفاظت نشود و بعد از تاریخ انقضا فاش گردد. تهدید حریم خصوصی مشابهی را ارائه می‌کند. سامانه امنیت و حفظ حریم خصوصی باید ذخیره‌سازی امن و واپایش دسترسی به بایگانی و پشتیبانی داده شامل اطلاعات شخصی زیست‌سنجشی و غیره را اداره کند.

۶-۴-۶ در معرض گذاری

در مواقع زیر، سازمان یا شخص سوم که اطلاعات زیست‌سنجشی برای آن‌ها فاش شده است (اطلاعات فاش شده در اختیار این سازمان یا شخص شوم قرار گرفته است) باید اطلاعات زیست‌سنجشی موضوع را به‌طور امن امحا کند (یادآوری می‌شود که این فهرست جامع نیست):

- هدفِ جمع‌آوری اطلاعات زیست‌سنجشی، به دست آمده است یا تعیین شده است که دیگر نیازی به آن نیست.
- دوره زمانی نگهداری اطلاعات زیست‌سنجشی منقضی شده است.
- موضوع رضایت خود برای جمع‌آوری یا استفاده از اطلاعات زیست‌سنجشی را پس می‌گیرد ولی موضوع اطلاعات زیست‌سنجشی راضی به استفاده جدید نیست.

در هنگام افشای اطلاعات زیست‌سنجشی ذخیره‌شده، اطمینان از اینکه داده‌های مناسب مرتبط شناسایی و به‌طور امن فاش شده‌اند، به‌خصوص در موارد ذخیره توزیع شده ضروری است. سامانه امنیت و حفظ حریم خصوصی باید اطلاعات شخصی زیست‌سنجشی و غیره که در فهرست داده می‌باشند را برای فاش‌سازی معین کند. این مورد باید شامل بایگانی و پشتیبانی داده باشد (برای جزئیات بیشتر به بند قبل مراجعه شود). همچنین حفاظت باید روش‌های اجرایی و حراست‌های مناسب را برای اطمینان از افشاسازی امن و کامل داده، توضیح دهد.

۶-۵ مسئولیت‌های صاحب سامانه زیست‌سنجشی

صاحب سامانه زیست‌سنجشی باید مسئول مدیریت مناسب اطلاعات زیست‌سنجشی به منظور حفاظت اطلاعات و حراست از حقوق موضوع در مورد اطلاعات زیست‌سنجشی در سازمان باشد. برای تامین این التزامات صاحب سامانه زیست‌سنجشی باید:

- موضوعی به‌وسیله واپایش اطلاعات زیست‌سنجشی او در طی چرخه زندگی‌اش و در هنگام تامین این اطلاعات برای شخص سوم را تامین کند؛ یعنی صاحب سامانه زیست‌سنجشی باید در هنگام جمع‌آوری اطلاعات زیست‌سنجشی، رضایت موضوع را به دست آورد.
- باید راهکاریی برای بازپس‌گیری رضایت تامین کند. موضوع می‌تواند پس گرفتن رضایتش را از یک سازمان یا شخص سومی که اطلاعات زیست‌سنجشی را به دست آورده است هرگاه احساس نیاز کند، درخواست نماید. مگر قوانین کاربردپذیر، آیین‌نامه‌ها یا اصطلاحات و شرایط خدمات

تعریف‌شده. صاحب سامانه زیست‌سنجشی باید وسایل مناسبی برای موضوع تامین کند تا بتواند چنین درخواستی مبنی بر حذف اطلاعات زیست‌سنجشی متناظر از سامانه زیست‌سنجشی را داشته باشد.

- اندازه‌گیری‌های امنیتی مناسبی برای حراست در برابر حملات به محرمانگی، یکپارچگی و در دسترس بودن اطلاعات زیست‌سنجشی و سامانه زیست‌سنجشی مرتبط را تامین کند.
- اطمینان یابد که اطلاعات استفاده‌شده برای شناسایی و درستی سنجی تصمیمات با احتمال وسیعی کامل، دقیق و به‌روز هستند. در این مورد عبارت اطلاعات مربوط به PII کلی، همچنین اطلاعات زیست‌سنجشی مربوط به موضوع است.
- مراجع زیست‌سنجشی بی‌کیفیت می‌توانند منجر به پذیرش حمله‌کننده توسط سامانه شود که روی حریم خصوصی موضوع تاثیر می‌گذارد.
- مسئول هرگونه درخواستی از طرف موضوع برای دسترسی به اطلاعات زیست‌سنجشی خود باشد. موضوع می‌تواند از صاحب سامانه زیست‌سنجشی بخواهد اجازه مشاهده اطلاعات زیست‌سنجشی خود را بدهد تا معیارهایی برای جزئیات استفاده از اطلاعات زیست‌سنجشی یا انتقال آن ها به شخص سوم را ایجاد کند و اصرار به تصحیح هر خطایی در اطلاعات، در صورت لزوم داشته باشد.
- اعلانِ هر گونه نَشت که منجر به نقض اطلاعات زیست‌سنجشی موضوع می‌شود را تامین کند. صاحب سامانه زیست‌سنجشی باید موضوع را از هر نقض شامل سرقت[1]، از بین رفتن[2]، آسیب[3]، افشاسازی غیرمجاز یا اصلاح غیرمجاز اطلاعات زیست‌سنجشی او آگاه سازد.

۷ الگوهای کاربردی سامانه زیست‌سنجشی و امنیت

۷-۱ الگوهای کاربردی سامانه زیست‌سنجشی

سامانه‌های زیست‌سنجشی می‌توانند به‌وسیله در نظر گرفتن مکان‌هایی که مراجع زیست‌سنجشی و مراجع شناسه ذخیره و مقایسه شده‌اند، همان‌طور که در جدول ۵ نشان داده شده است، طبقه‌بندی شوند. در اصطلاح امنیت، هر الگو مزیت‌ها و معایب معینی در رابطه با مدیریت مراجع زیست‌سنجشی و مراجع شناسه در هنگام انتقال یا ذخیره‌سازی آن ها دارد. به‌طور مفهومی، الگوهای زیادی وجود دارند؛ به هر حال این استاندارد ۸ نوع از مدل‌ها را در نظر می‌گیرد که در حال حاضر در کاربردهای واقعی به کار می‌روند.

جدول ۵- الگوی کاربرد یک سامانه زیست‌سنجشی

1 - Theft
2 - Loss
3 - Damage

		ذخیره‌سازی			
		کارساز	کارخواه	نمودافزار	توزیع شده
مقایسه	کارساز	A		B	G
	کارخواه	C	D	E	H
	نمودافزار			F	

مکان‌ها می‌توانند به‌صورت زیر شرح داده شوند:

- یک کارساز رایانه‌ای است که از دور از طریق شبکه به کارخواه متصل است. «یک کارساز اصالت-سنجی زیست‌سنجشی» شکلی از کارساز است.
- یک کارخواه، رایانه شخصی یا معادل آن است که هدف کلی سامانه بهره‌برداری را اجرا می‌کند و می‌تواند به شکل یک دکه باشد. ویژگی‌های اساسی یک کارخواه آن است که اول تا آخر خدمات برای سامانه زیست‌سنجشی را تامین کند و رابط کارساز و / یا نمودافزار باشد. یک واحد حسگر زیست‌سنجشی می‌تواند به کارخواه متصل یا در آن جاسازی شود. در این استاندارد PDA ها و گوشی‌های همراه هوشمند معین به عنوان کارخواه در نظر گرفته می‌شوند.
- یک نمودافزار افزاره فیزیکی قابل‌حمل است که توانایی پشتیبانی ذخیره مراجع زیست‌سنجشی را دارد و در برخی موارد اجازه مقایسه زیست‌سنجشی می‌دهد.

نمودافزارها برای ذخیره‌سازی زیست‌سنجشی‌ها شامل کارت حافظه USB، گذرنامه‌های الکترونیکی و کارت‌های هوشمند می‌شوند. کارت‌های هوشمند می‌توانند برای مقایسه و تصمیم‌گیری زیست‌سنجشی، کاربر مقایسه روی کارت را درست کنند.

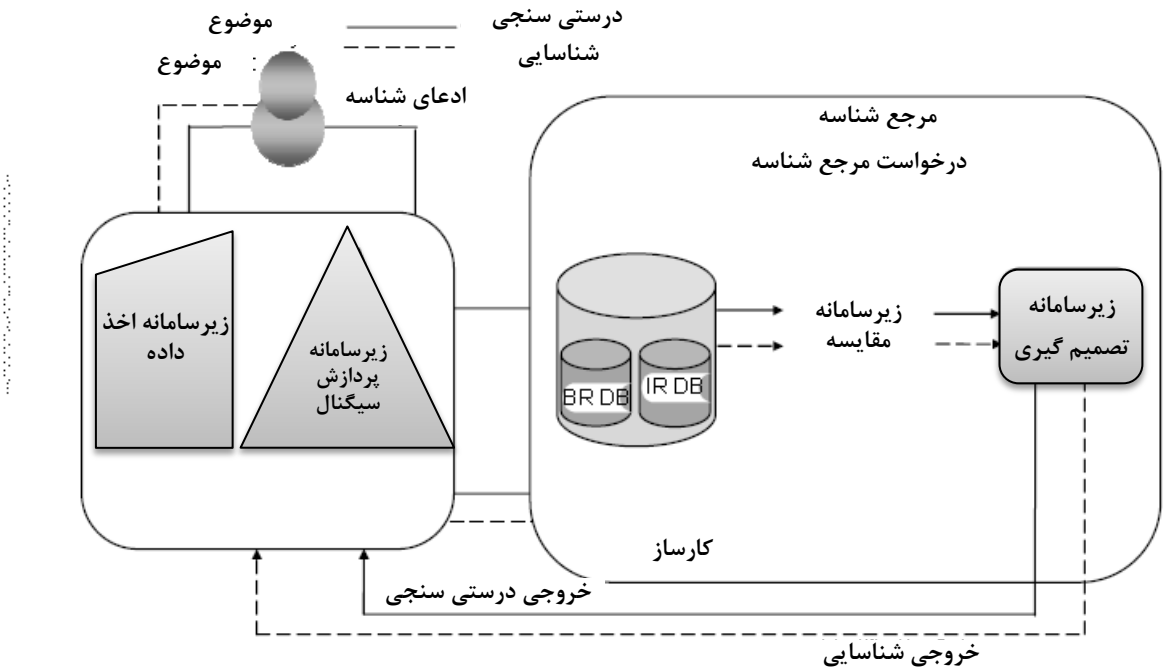
یادآوری- حسگر زیست‌سنجشی از طریق نمونه حسگر میانجی به کارخواه متصل می‌شود و یک نمونه حسگر جاسازی‌شده در کارخواه می‌تواند به عنوان سایر مکان‌ها برای ذخیره‌سازی و مقایسه در نظر گرفته شود. به هر حال کارخواه‌ها به‌طور متواتر با حسگرهای زیست‌سنجشی تجهیز شده‌اند. این استاندارد آن ها را به عنوان بخشی از کارخواه در نظر می‌گیرد.

در ادامه الگوهای A تا F، مکان‌شناسی‌های متفاوتی برای مکان‌های زیرسامانه‌های متنوع شرح می‌دهند. الزامات امنیتی، یک معیار خواهند بود که تعیین می‌کنند مراجع زیست‌سنجشی عادی یا تجدیدپذیر باید استفاده شوند؛ به عبارت دیگر الگوهای G و H فقط برای مراجع زیست‌سنجشی تجدیدپذیر (RBR ها) به کار می‌روند زیرا این الگوها مفهوم جداسازی داده PI و AD را به‌وسیله توزیع ذخیره‌سازی در میان سامانه‌های ذخیره‌سازی چندگانه برای بالا بردن امنیت و حریم خصوصی سامانه‌های زیست‌سنجشی، به کار می‌گیرند. به دلیل این جداسازی داده، الگوهای G و H فقط برای فرایند درستی سنجی به کار می‌روند.

۲-۷ امنیت در هر مدل کاربردی زیست‌سنجشی

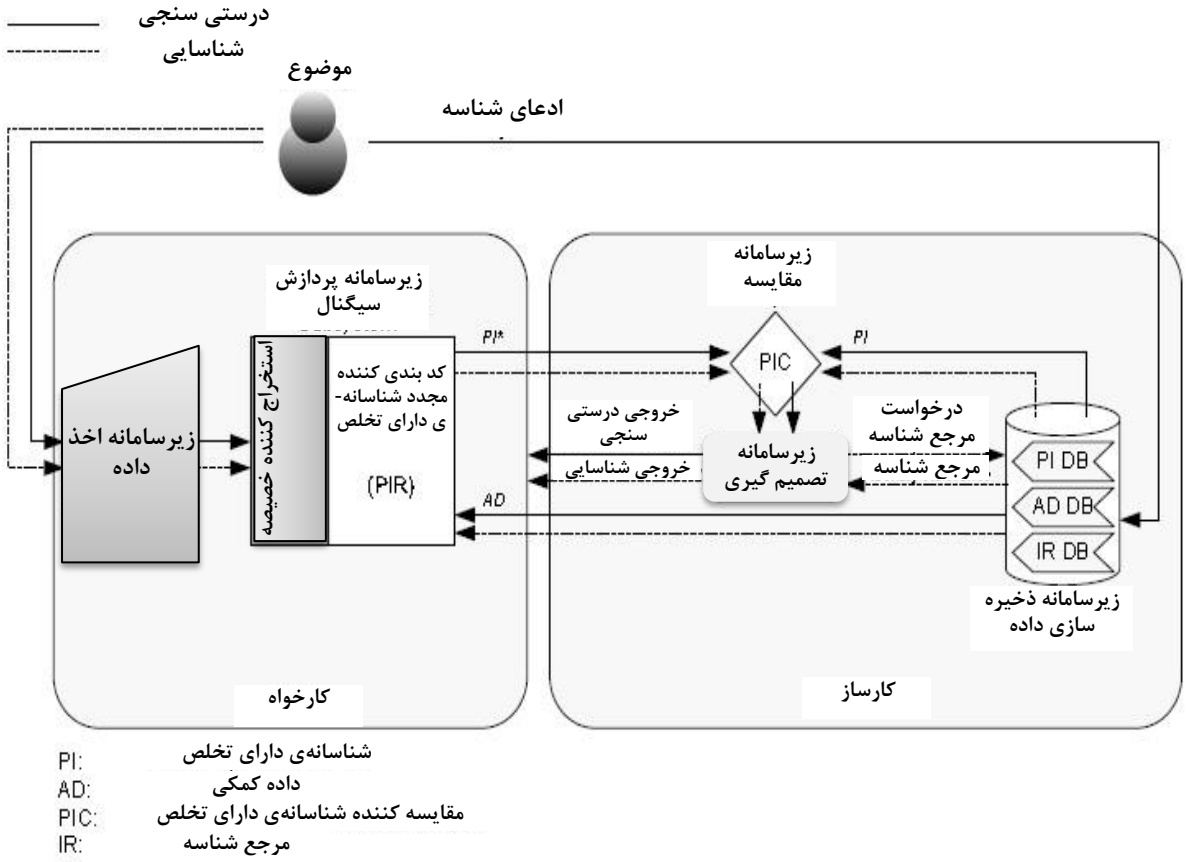
۱-۲-۷ الگوی A – ذخیره در کارساز و مقایسه در کارساز

در این الگو، مراجع زیست‌سنجشی در کارساز ذخیره‌شده‌اند و نیاز است که داده زیست‌سنجشی برای مقایسه به کارساز انتقال یابد، همان‌طور که در شکل ۶ (برای BR ها) و شکل ۷ (برای RBR ها) نشان داده شده است. مرجع زیست‌سنجشی موضوع و مرجع شناسه متناظر با آن به عنوان یک بخش از فرایند ثبت‌نام / ثبت مرتبط شده‌اند.



شکل ۶- الگوی A – ذخیره در کارساز و مقایسه در کارساز با استفاده از USB

این الگو نیاز دارد که کارساز به داده اخذشده از کارخواه اعتماد کند. این الگو می‌تواند برای شناسایی و همچنین درستی سنجی استفاده شود. از آن جایی که PII حساس (به عنوان مثال مرجع زیست‌سنجشی و مرجع شناسه) به‌وسیله کارساز سامان‌دهی شده است، امنیت دادگان قابل‌اعتماد و امنیت شبکه الزامی است. یک سامانه بزرگ تجاری شناسایی اثرانگشت خودکار (AFIS) بیشتر اوقات مطابق با این الگو پیاده‌سازی می‌شود. از نقطه نظر حریم خصوصی، در بیشتر اوقات این الگو پیشنهاد نمی‌شود، مگر در موردی که مراجع زیست‌سنجشی تجدیدپذیر که توسط شکل ۷ با نمونه نشان داده شده است، به کار گرفته شود، به دلیل PII حساس که در یک دادگان متمرکز جمع‌آوری‌شده است.



شکل ۷- الگوی A – ذخیره در کارساز و مقایسه در کارساز با استفاده از RBR ها

۷-۲-۲ الگوی R – ذخیره در نمودافزار و مقایسه در کارساز

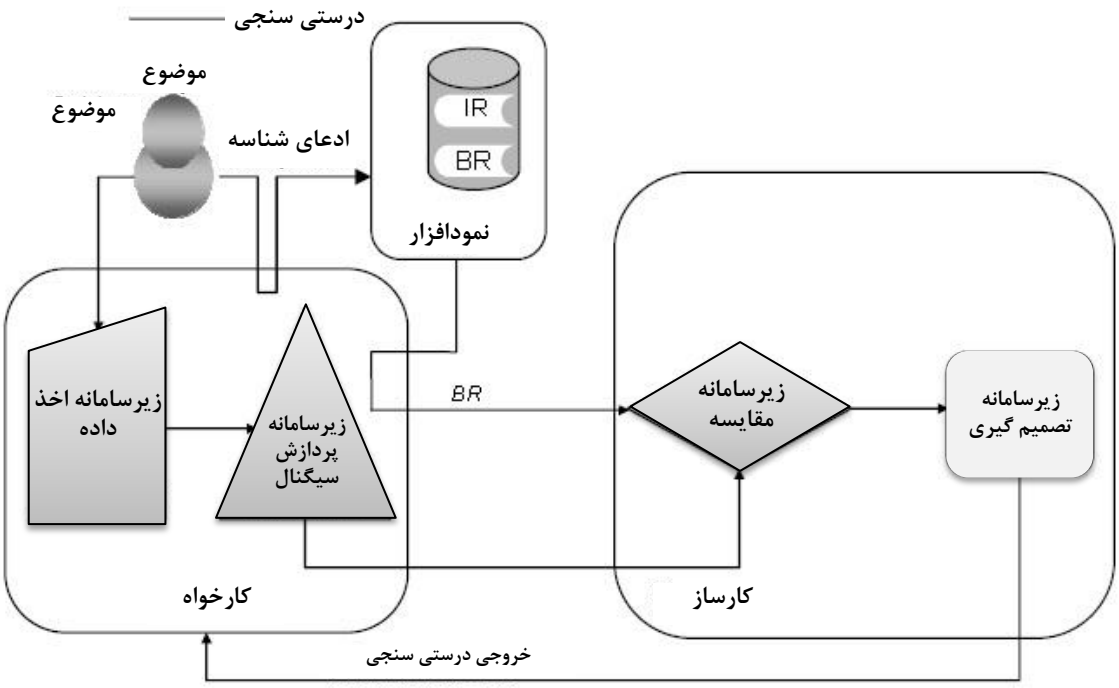
در این الگو، یک نمودافزار برای ذخیره‌سازی مراجع زیست‌سنجشی استفاده می‌شود و نیاز دارد که داده‌های زیست‌سنجشی اخذشده برای مقایسه به کارساز انتقال یابند، همان‌طور که در شکل ۸ و ۹ نشان داده شده است.

موضوع زیست‌سنجشی در طی فرایند ثبت، مرجع زیست‌سنجشی خود را با مرجع شناسه در یک نمودافزار مرتبط می‌کند. توصیه می‌شود یک موضوع که می‌خواهد از شناسه خود دفاع کند، نمودافزار داشته باشد و آن را به کارخواه متصل کند و همچنین مشخصه‌های زیست‌سنجشی خود را ارائه دهد.

سپس کارخواه هم مرجع زیست‌سنجشی ذخیره‌شده و هم خصیصه زیست‌سنجشی اخذشده را برای مقایسه به کارساز می‌فرستد.

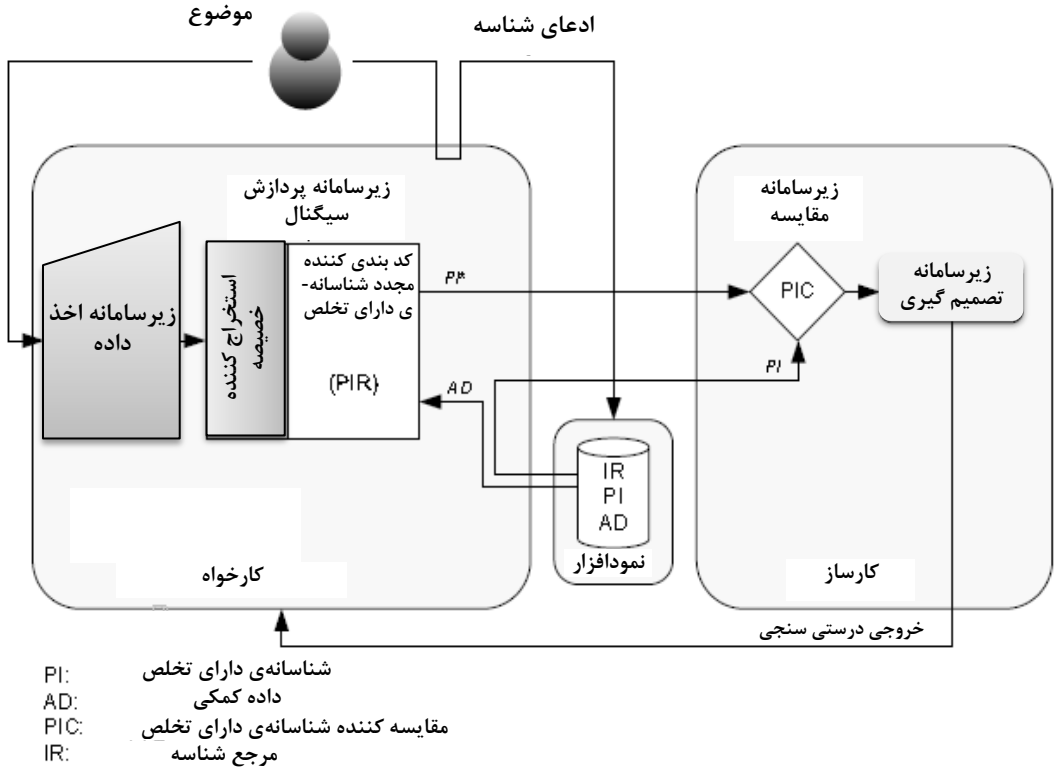
در مورد RBR ها، PI که در طی ثبت تولیدشده و سپس در نمودافزار ذخیره‌شده است و شناسانه‌ی دارای

تخلص داوطلب (PI*)[1] که در طی درستی سنجی نوسازی شده است به کارساز فرستاده می‌شوند، در حـالی که AD فقط برای کارخواه تامین شده است. همچنین این الگو می‌تواند با ذخیره‌سازی PI ها در نمـودافزار و کارساز گسترده شود تا اصالت‌سنجی سه عامل را مجاز کند.



شکل ۸- الگوی B، ذخیره در نمودافزار و مقایسه در کارساز با استفاده از BR ها

1 - Candidate pseudonymous identifier



شکل ۹- الگوی B، ذخیره در نمودافزار و مقایسه کارساز با استفاده از RBR ها

این مدل نیاز دارد که کارساز به داده اخذشده از کارخواه اعتماد کند. در بیشتر اوقات این مدل برای درستی سنجی استفاده می‌شود زیرا مرجع زیست‌سنجشی دیگری برای مقایسه در نمودافزار وجود ندارد به‌جز آن که توسط اشخاص ادعا می‌گردد. از آن جایی که مرجع زیست‌سنجشی در نمودافزار قابل‌حمل ذخیره‌شده است، که می‌تواند به طرز امن توسط اشخاص حمل شود، این الگو نیاز به امنیت دادگان ندارد. به هر حال این الگو نیاز به امنیت شبکه برای حفاظت انتقال مرجع زیست‌سنجشی ذخیره‌شده و داده زیست‌سنجشی کاوشگر اخذشده دارد. این مورد برای اطمینان داشتن از این است که کارساز بتواند مطمئن باشد که داده مرجع از طرف ریشه‌های کارخواه از فرایند ثبت آمده نه اینکه بلافاصله قبل از درستی سنجی در شبکه گذاشته شده باشد. یادآوری می‌شود که مرجع شناسه در کارخواه یا کارساز، نه منتقل شده و نه با مرجع زیست‌سنجشی پیوند دارد؛ بنابراین این الگو می‌تواند به عنوان الگوی موافق حریم خصوصی در نظر گرفته شود.

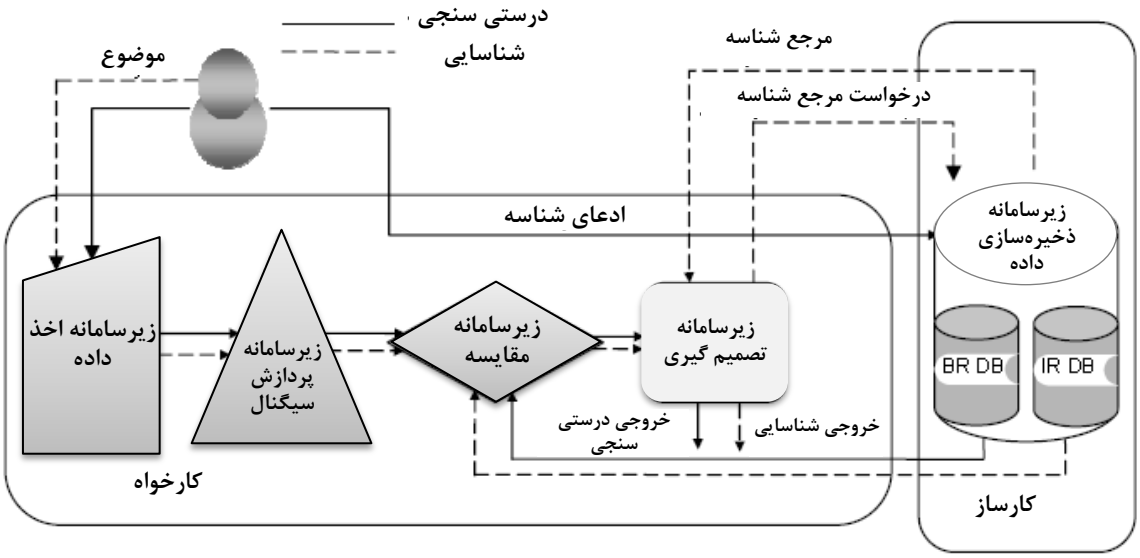
۳-۲-۷ الگوی C – ذخیره در کارساز و مقایسه در کارخواه

در این الگو مراجع زیست‌سنجشی در کارساز ذخیره می‌شوند و داده زیست‌سنجشی کاوشگر در طرف کارخواه برای فرایند مقایسه از موضوع استخراج می‌گردد. همان‌طور که در شکل ۱۰ و ۱۱ نشان داده شده، موضوع زیست‌سنجشی مرجع زیست‌سنجشی خود را با مرجع شناسه در کارساز در طی فرایند ثبت، مرتبط می‌کند.

یک موضوع که می‌خواهد شناسه خود را ادعا کند نمونه زیست‌سنجشی کاوشگرش را به کارخواه ارائه

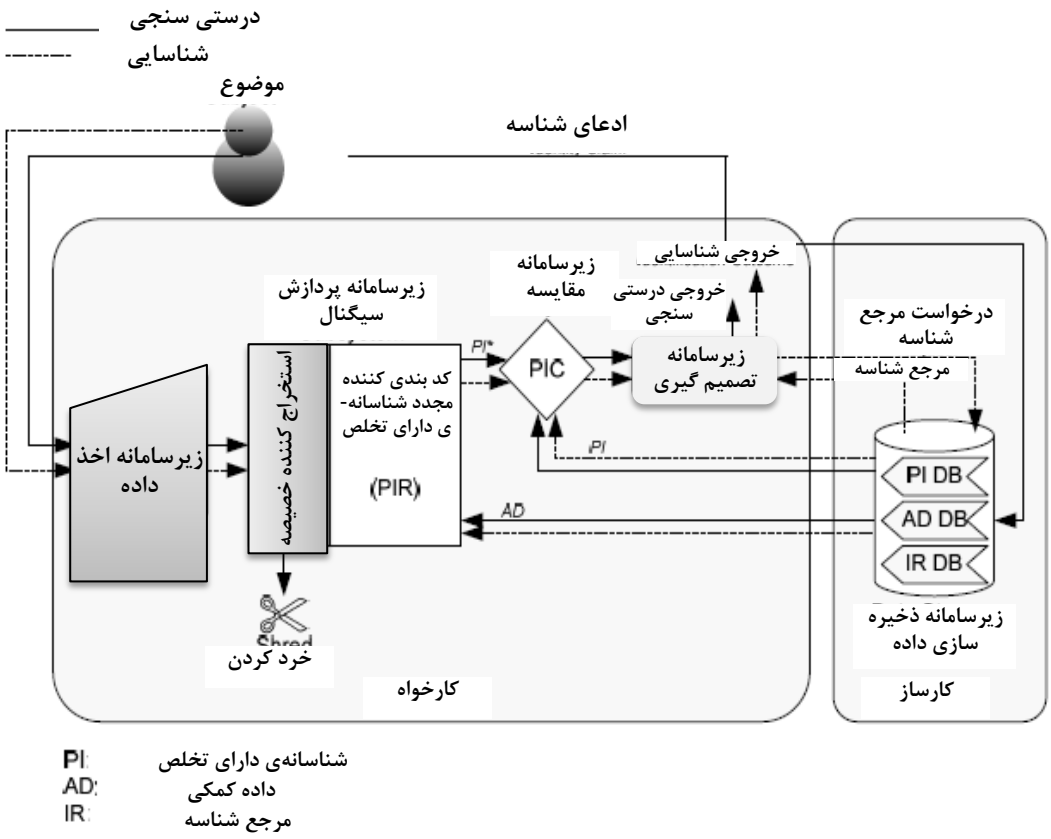
می‌دهد و سپس کارخواه درخواست فرستادن مرجع زیست‌سنجشی متناظر مربوط به موضوع زیست‌سنجشی ادعا شده را می‌نماید. به‌محض اینکه درخواست انجام شد، کارساز مرجع زیست‌سنجشی ادعا شده را به کارخواه می‌فرستد و سرانجام کارخواه مقایسه‌ای بین نمونه زیست‌سنجشی اخذشده و مرجع زیست‌سنجشی بارگیری شده انجام می‌دهد.

برای این الگو، کارخواه باید مجهز به حسگر زیست‌سنجشی و همچنین الگوریتم مقایسه / تصمیم‌گیری باشد.



شکل ۱۰- الگوی C – ذخیره در کارساز و مقایسه در کارخواه با استفاده از BR ها

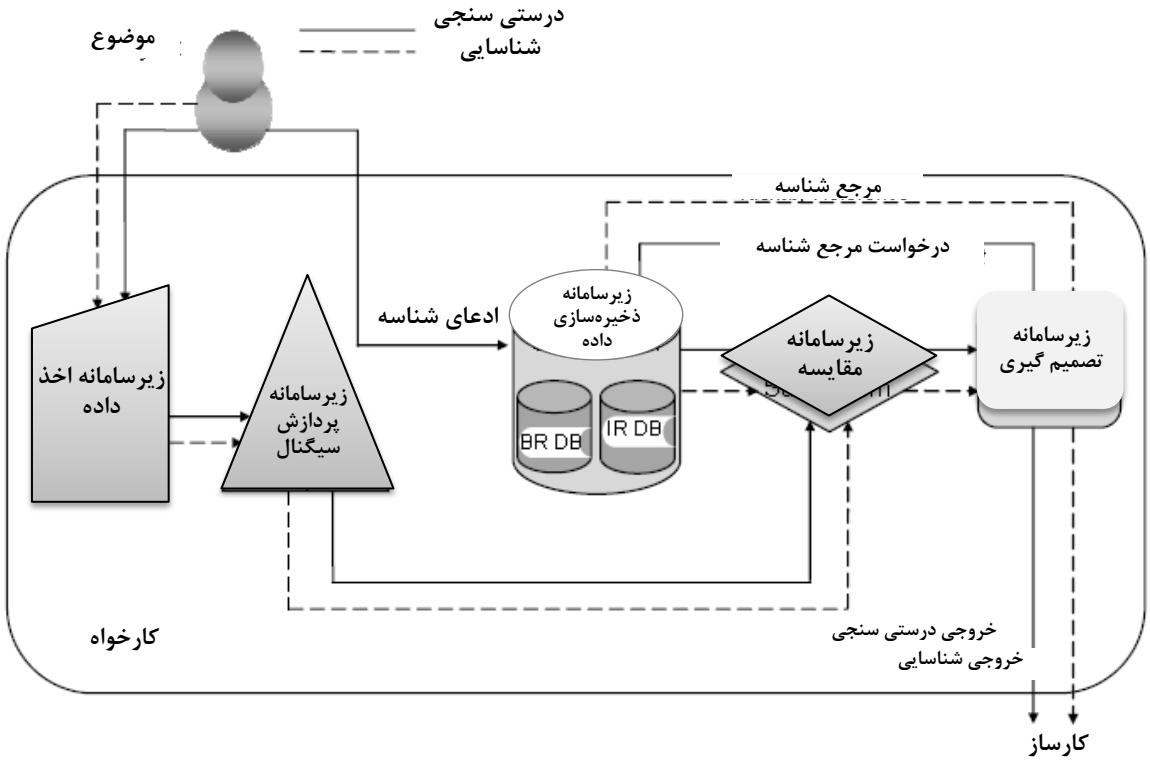
این مدل نیاز به اطمینان از این دارد که داده از کارساز به دست آید. این مدل می‌تواند برای شناسایی و همچنین درستی سنجی استفاده شود. از آنجایی که PII حساس (به عنوان مثال مراجع زیست‌سنجشی و مراجع شناسه) در بیشتر اوقات در کارساز متمرکز ذخیره می‌شوند، امنیت دادگان و امنیت شبکه قابل‌اعتماد برای حراست از حریم شخصی موضوع زیست‌سنجشی مورد نیاز است.



شکل ۱۱- الگوی C – ذخیره در کارساز و مقایسه در کارخواه با استفاده از RBR ها

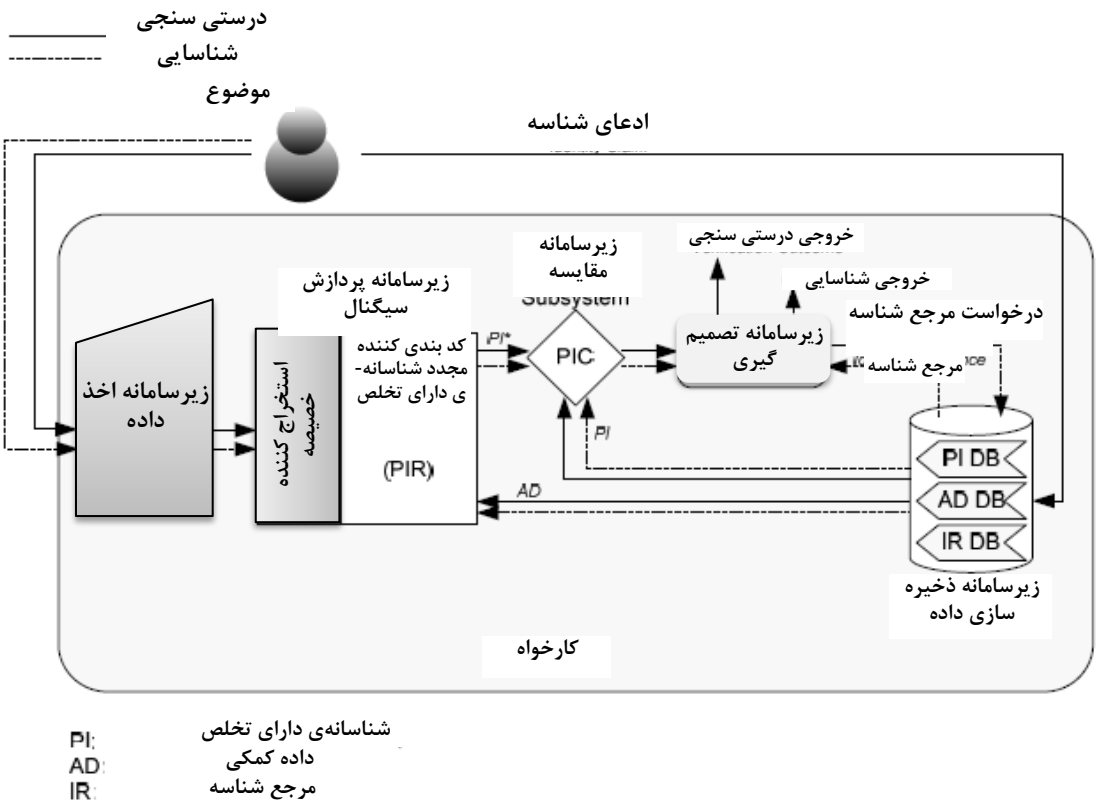
۴-۲-۷ الگوی D – ذخیره در کارخواه و مقایسه در کارخواه

در این الگو، مراجع زیست‌سنجشی در کارخواه ذخیره‌شده‌اند و نمونه زیست‌سنجشی کاوشگر از موضوع زیست‌سنجشی برای فرایند مقایسه استخراج می‌شود که مطابق با شکل ۱۲ و ۱۳ در کارخواه اجرا می‌گردد. موضوع مرجع زیست‌سنجشی خود را با مرجع شناسه در کارخواه در طی فرایند ثبت مرتبط می‌کند. برای گسترش دادن این الگو، کارخواه باید مجهز به حسگر زیست‌سنجشی و یک الگوریتم مقایسه / تصمیم‌گیری باشد. این مدل در بیشتر اوقات برای اصالت‌سنجی موضوعات به کار می‌رود که از افزاره‌هایی مثل رایانه‌های رومیزی شخصی و تلفن‌های همراه استفاده می‌کند. در برخی موارد کارخواه می‌تواند در حالتی مستقل عمل کند که نیاز به اتصال با کارساز نیست. در سایر موارد، اصالت‌سنجی نهایی می‌تواند به‌وسیله کارسازی که نتایج درستی سنجی داده شده توسط کارخواه را تایید می‌کند، ساخته شود.



شکل ۱۲- الگوی D – ذخیره در کارخواه و مقایسه در کارخواه با استفاده از BR ها.

این مدل می‌تواند برای شناسایی و درستی سنجی به کار رود. از آن جایی که PII حساس (به عنوان مثال مراجع زیست‌سنجشی و مراجع شناسه) به کارساز منتقل نمی‌شوند، مسئولیت امنیت شبکه می‌تواند کمینه شود، اگرچه امنیت دادگان قابل‌اعتماد همچنان برای کارخواه مورد نیاز است و بنابراین مراجع زیست-سنجشی تجدیدپذیر پیشنهاد می‌شوند. در مورد حریم خصوصی، این مدل بیشتر از سایر الگوهایی که از دادگان متمرکز استفاده می‌کنند مطلوب است.

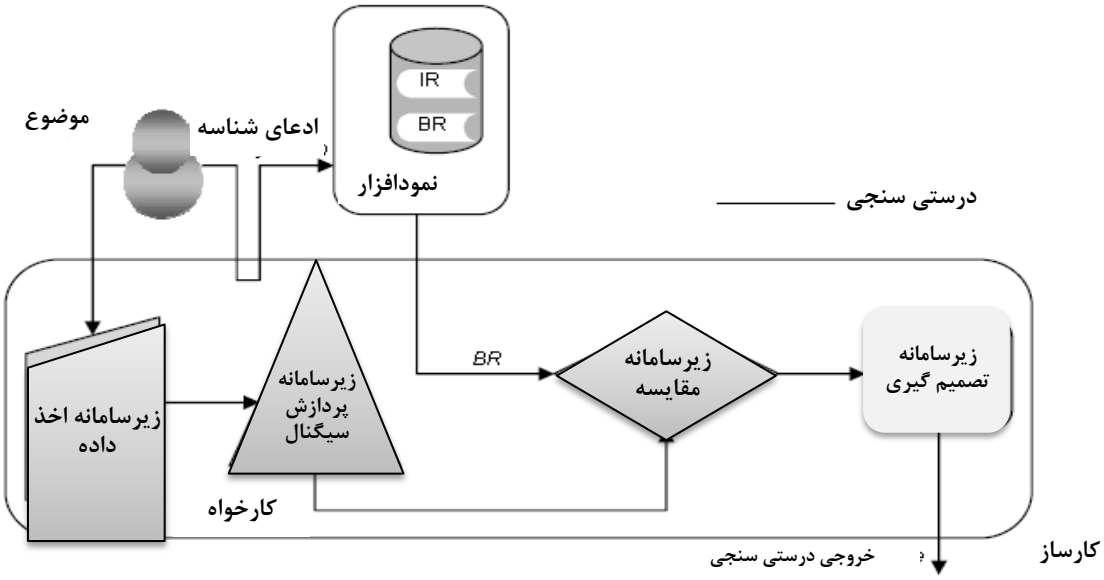


شکل ۱۳- الگوی D – ذخیره در کارخواه و مقایسه در کارخواه با استفاده از RBR ها

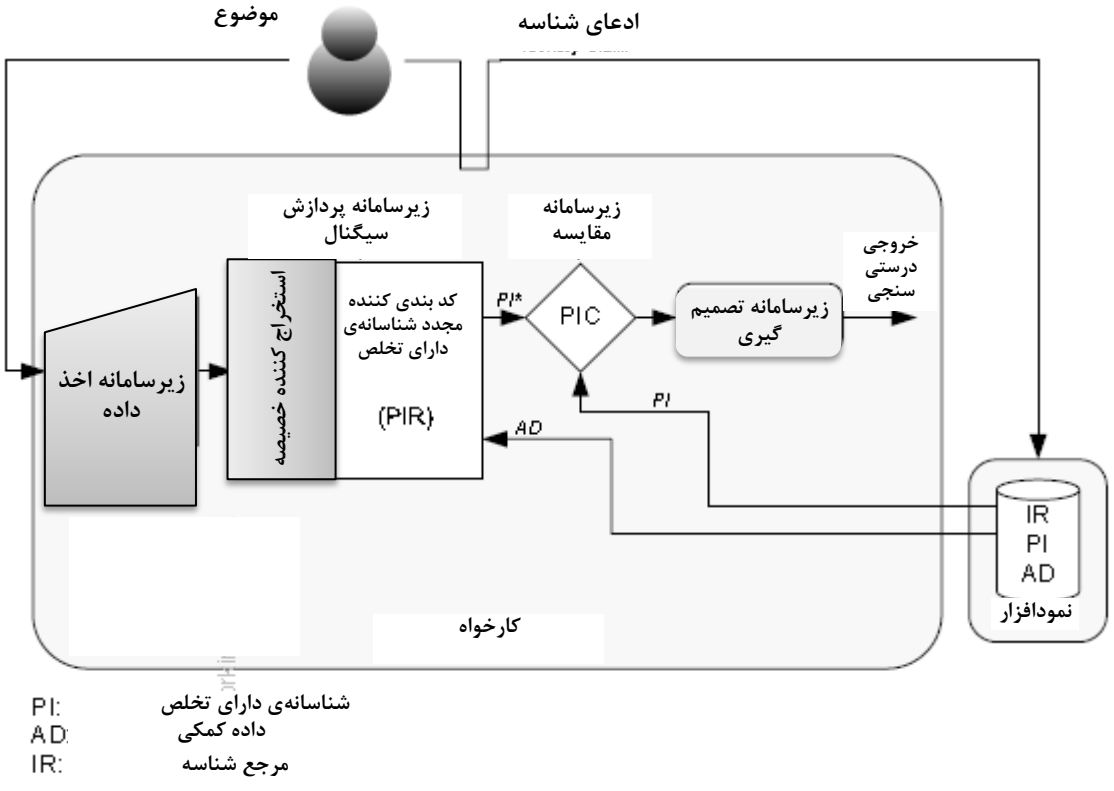
۵-۲-۷ الگوی E – ذخیره در نمودافزار و مقایسه در کارخواه

در این الگو مراجع زیست‌سنجشی در نمودافزار ذخیره‌شده‌اند و یک نمونه زیست‌سنجشی کاوشگر از موضوع برای فرایند مقایسه که در کارخواه اجرا می‌شود و در شکل‌های ۱۴ و ۱۵ نشان داده شده است، استخراج می‌شود.

موضوع زیست‌سنجشی مرجع زیست‌سنجشی خود را با مرجع شناسه در نمودافزار در طی فرایند ثبت مرتبط می‌کند. یک موضوع که می‌خواهد شناسه خود را ادعا کند باید نمونه زیست‌سنجشی کاوشگر خود را با نمودافزار و مرجع زیست‌سنجشی ذخیره‌شده در آن به کارخواه ارائه دهد. برای گسترش این الگو، کارخواه باید مجهز به حسگر زیست‌سنجشی و نرم‌افزار پردازش شامل الگوریتم مقایسه / تصمیم‌گیری باشد. در اینجا کارخواه می‌تواند نوع دکه باشد، همان‌طور که در مکان‌های عمومی مثل فرودگاه و ساختمان‌های عمومی برای اصالت‌سنجی شخصی پیدا می‌شود. این الگو در واپایش مرز با استفاده از گذرنامه الکترونیکی به عنوان نمودافزار به کار می‌رود.



شکل ۱۴- الگوی E – ذخیره در نمودافزار و مقایسه در کارخواه با استفاده از BR ها



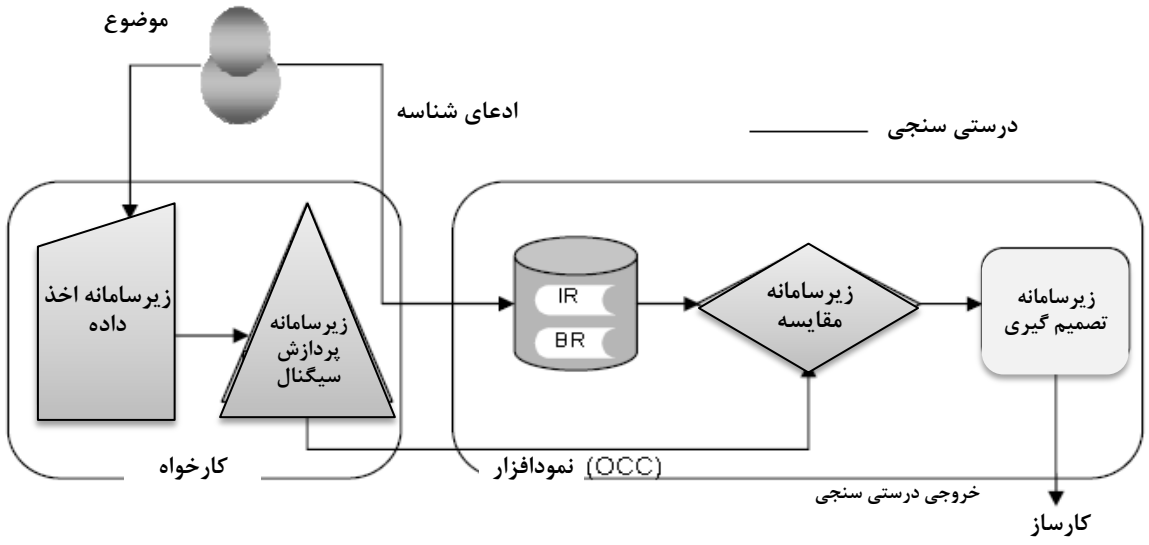
شکل ۱۵- الگوی E – ذخیره در نمودافزار و مقایسه کارخواه با استفاده از RBR ها

مراجع زیست‌سنجشی و مراجع شناسه می‌توانند در یک تراشه IC جاسازی‌شده در یک نمودافزار ذخیره شوند. این الگو در بیشتر مواقع برای درستی سنجی به کار می‌رود. از آنجایی که PII حساس (به عنوان مثال مرجع زیست‌سنجشی و مرجع شناسه) به کارساز منتقل نمی‌شوند، مسئولیت امنیت شبکه می‌تواند کمینه شود اگرچه همچنان نیاز به امنیت دادگان قابل‌اعتماد است. در مورد حریم خصوصی، این الگو بیشتر از سایر الگوهایی که برای مرجع زیست‌سنجشی و شناسه از ذخیره‌سازی متمرکز استفاده می‌کنند، مطلوب است. توصیه می‌شود فرمان خطاب شده به نمودافزار برای خواندن مرجع زیست‌سنجشی و پاسخگویی متعاقب به‌وسیله نمودافزار که داده مرجع زیست‌سنجشی را حمل می‌کند، با استفاده از راهکار پیام‌رسانی امن مطرح شده در استاندارد ISO /IEC 7816-4 امن بماند.

۶-۲-۷ الگوی F – ذخیره در نمودافزار و مقایسه در نمودافزار

در این الگو مراجع زیست‌سنجشی در نمودافزار ذخیره می‌شوند و نمونه زیست‌سنجشی کاوشگر از موضوع زیست‌سنجشی برای فرایند مقایسه که مطابق با شکل ۱۶ در نمودافزار اجرا می‌شود، استخراج می‌گردد.

موضوع مرجع زیست‌سنجشی خود را با مرجع شناسه در نمودافزار و در طی فرایند ثبت مرتبط می‌کند. یک موضوع که می‌خواهد شناسه خود را ادعا کند باید نمونه زیست‌سنجشی کاوشگرش را با نمودافزار به کارخواه ارائه دهد (مقایسه روی کارت). برای گسترش این الگو، نمودافزار باید مجهز به الگوریتم مقایسه / تصمیم‌گیری باشد. در اینجا، کارخواه باید دستگاه خودپرداز (ATM) باشد. این الگو در بیشتر مواقع برای انتقالات بانکی با استفاده از OCC به کار می‌رود.

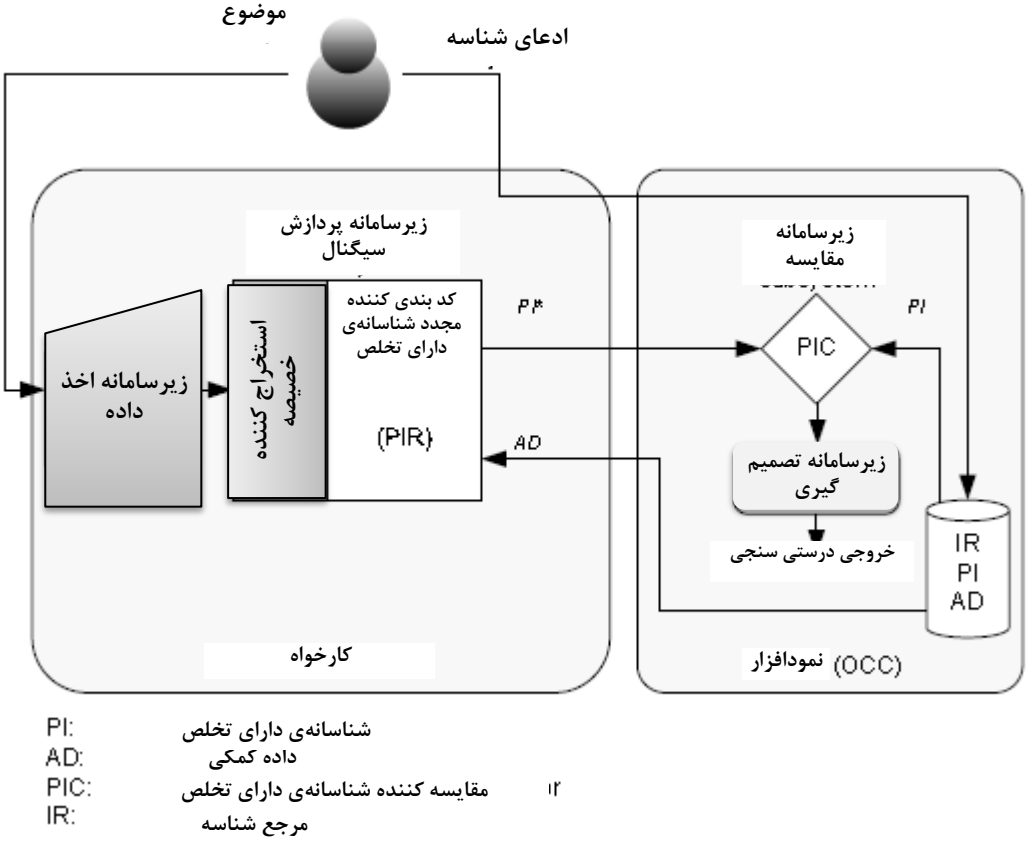


شکل ۱۶- الگوی F – ذخیره در نمودافزار و مقایسه در نمودافزار با استفاده از BR ها

این نوع از الگو OCC قوی‌ترین راهکار برای حفاظت اطلاعات شخصی است. نمودافزار BR و IR را ذخیره

می‌کند و فرایند مقایسه هم در کارت اجرا می‌شود.
نمودافزار باید توانایی خود اجرایی را داشته باشد. توصیه می‌شود فرمان خطاب شده بـه کـارت بـرای شـروع فرایند مقایسه و پاسخ متعاقب به‌وسیله کارت که نتیجه فرایند مقایسه را حمل می‌کند، با استفاده از راهکـار پیام‌رسانی امن مطرح شده در استاندارد ISO /IEC 7816-4 امن باشد.
کارخواه نیاز به یک نمونه زیست‌سنجشی کاوشگر و داده IR دارد و آن ها را برای فرایند مقایسه به نمودافزار می‌فرستد. نتیجه مقایسه به کارساز فرستاده شده است. در اینجا نمـودافزار ممکـن اسـت حـاوی زیرسـامانه پردازش سیگنال باشد. در این مورد، احتمال نقض اطلاعات زیست‌سنجشی موضوع می‌تواند کاهش یابد.

این الگو افشای یک PII شخصی به‌وسیله ذخیره‌سازی مرجع زیست‌سنجشی و شناسه در نمودافزار را محدود می‌کند. به‌علاوه، برای RBR ها (به شکل ۱۷ مراجعه شود)، فقط AD به کارخواه منتقل شده است، در حالی که PI در نمودافزار باقی می‌ماند؛ بنابراین این الگو می‌تواند به عنوان یـک محـافظ حـریم خصوصـی در نظـر گرفته شود در حالی که اطلاعات زیست‌سنجشی تحت واپایش موضوع هستند. به هر حال همان‌طـور کـه در برخی الگوهای بالا گفته شد، گام‌های قابل‌اعتماد باید در ارتباط بـین کـارخواه و کارسـاز جاسـازی شـود در نتیجه کارساز می‌تواند اطمینان داشته باشد که اصالت‌سنجی موضوع داده نتیجه مقایسه خالص است. مکررا، زیرسامانه‌های اخذ داده و پردازش سیگنال هم می‌توانند در نمودافزار مجتمع شوند. شروط پیاده‌سازی الگوی F توسط استاندارد ISO /IEC 24787 (مقایسه زیست‌سنجشی در کارت) استانداردسازی شده است.



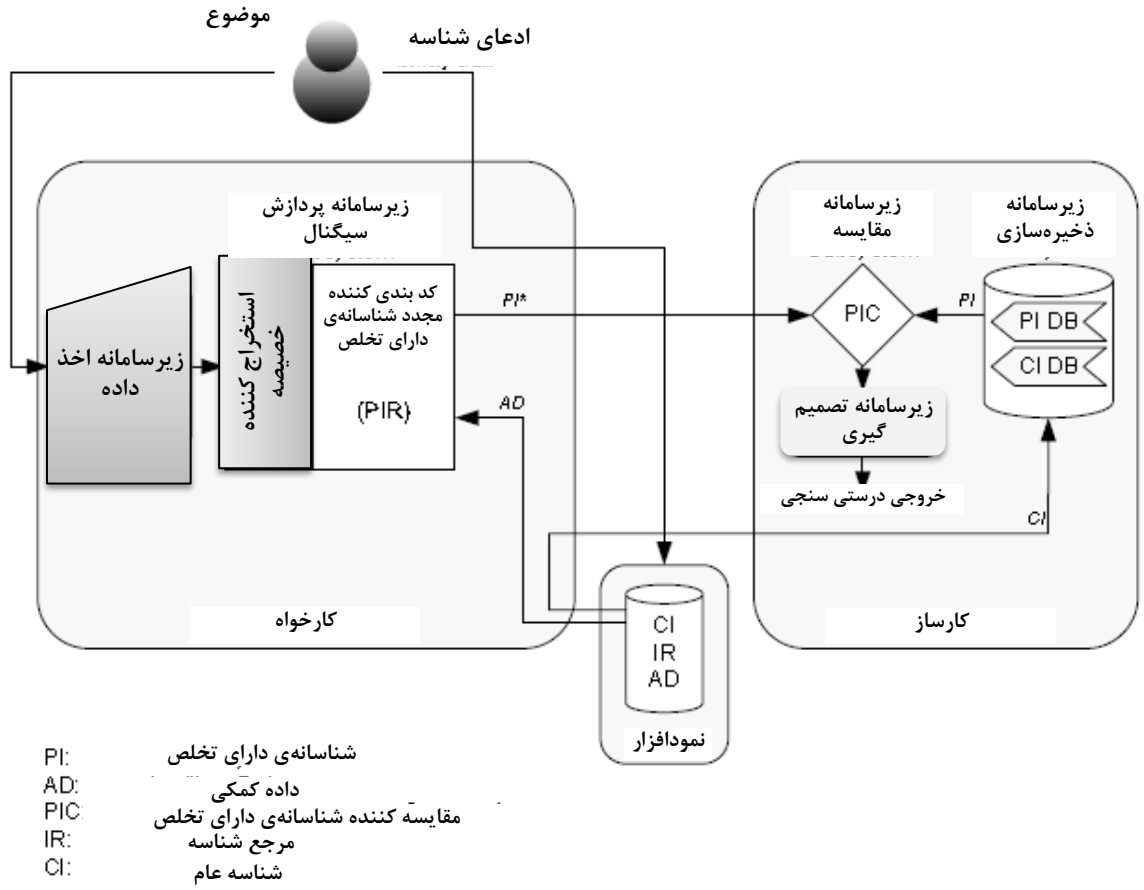
شکل ۱۷- الگوی F – ذخیره در نمودافزار و مقایسه در نمودافزار با استفاده از RBR ها

۷-۲-۷ الگوی G – ذخیره‌سازی توزیع شده در نمودافزار و کارساز، مقایسه در کارساز

این الگو جداسازی داده از طریق ذخیره‌سازی توزیع شده عناصر داده از RBR ها را به کار می‌گیرد. در طی فاز ثبت یک پیاده‌سازی از این الگو، یک شناسانه‌ی دارای تخلص ایجاد شده و در کارساز به‌وسیله شناسانه عام (CI) همراهی می‌شود. AD، IR و CI متناظر در نمودافزار ذخیره‌شده‌اند. در طی درستی سنجی، نمودافزار AD و CI را برای کارخواه انتشار می‌دهد (به شکل ۱۸ مراجعه شود). کارخواه داده زیست‌سنجشی کاوشگر را اخذ و آن را به *PI منتقل می‌کند. *PI و CI به کارساز منتقل شده‌اند. کارساز PI و *PI را مقایسه می‌کند که در خروجی درستی سنجی نتیجه می‌شود. یک مزیت مهم این الگو این است که مرجع زیست‌سنجشی تجدیدپذیر بین نمودافزار و کارساز توزیع شده است. درستی سنجی فقط وقتی امکان‌پذیر است که هم کارساز و هم نمودافزار حاوی داده صحیح باشند. این ویژگی مخاطره مداخله با مراجع زیست-سنجشی را کاهش می‌دهد زیرا او نیاز به مداخله با نمودافزار و همچنین داده در کارساز دارد. به‌علاوه اجازه ابطال‌پذیری داده مرجع زیست‌سنجشی (PI ها) در سمت کارساز بدون نیاز به دسترسی به نمودافزار را می‌دهد. مزیت سوم این است که موضوع بر فرایند درستی سنجی واپایش دارد زیرا نیاز به نمودافزاراش است. تنوعات و سازگاری‌های این الگو که در زیر آمده می‌تواند به کار گرفته شود:

- IR ذخیره‌شده در کارساز به جای نمودافزار
- ذخیره‌سازی CI، IR، AD در کارخواه و PI، CI در کارساز بدون نمودافزار
- ذخیره‌سازی PI در هم نمودافزار و هم کارساز برای مجاز کردن اصالت‌سنجی سه عامل در سمت کارساز. در این پیاده‌سازی PIC، PI را از زیرسامانه ذخیره‌سازی کارساز، PI را از نمودافزار و *PI نتیجه شده از PIR را دریافت می‌کند.

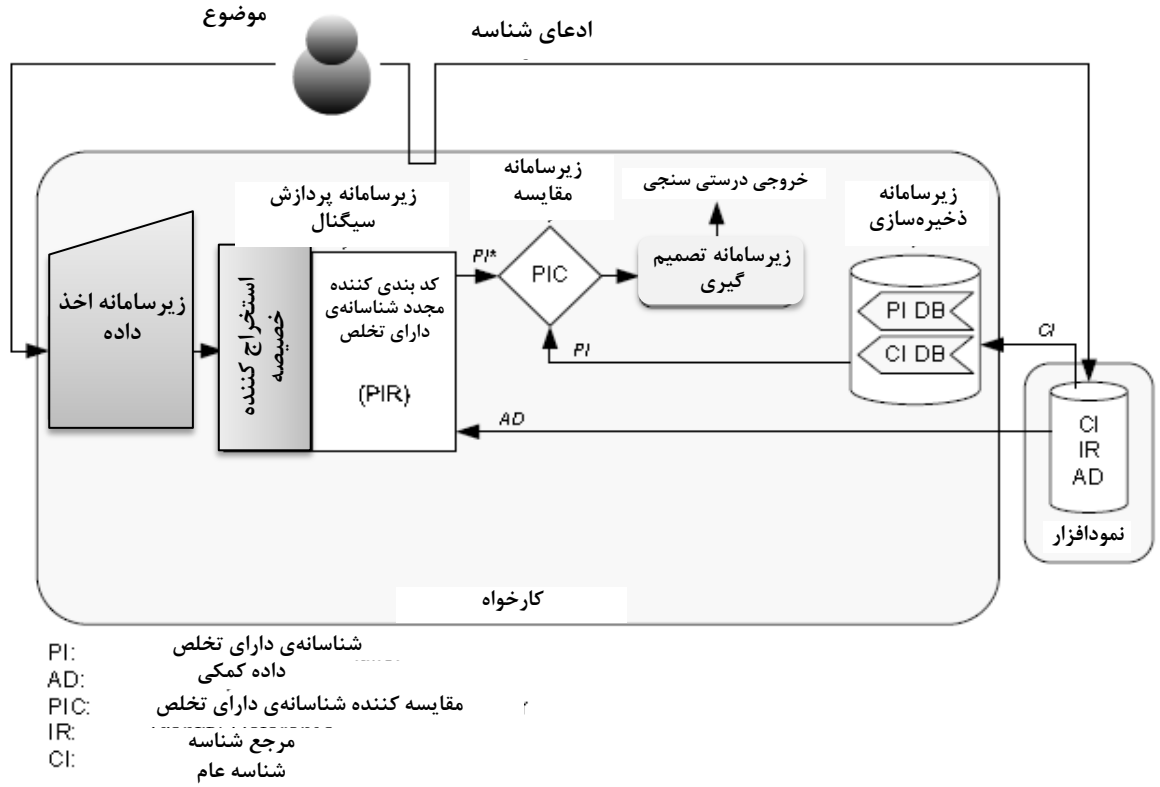
این الگو مخصوصاً برای اصالت‌سنجی تراکنش برخط (مثل بانکداری الکترونیکی، معاملات کارت اعتباری برخط و به عنوان جایگزین یا بالا برنده PIN برای ATM ها) که یک کارت یا نمودافزار که قادر به ذخیره‌سازی داده کمکی است، مناسب است. برای کمینه کردن مقدار تبادل اطلاعات بین کارخواه و کارساز و برای جلوگیری از انتقال بخش‌های داده RBR از کارساز به کارخواه، ذخیره PI در نمودافزار و AD در کارساز پیشنهاد نمی‌شود.



شکل ۱۸- الگوی G: ذخیره توزیع شده در نمودافزار و کارساز، مقایسه در کارساز

۸-۲-۷ الگوی H – ذخیره توزیع شده در نمودافزار و کارخواه، مقایسه در کارخواه

در این الگو، AD، IR و CI در نمودافزار ذخیره‌شده‌اند و PI و CI با کارخواه ذخیره‌شده‌اند (به شکل ۱۹ مراجعه شود). در طی درستی سنجی، نمودافزار CI و AD را به کارخواه انتشار می‌دهد. کارخواه PI متناظر با CI را از زیرسامانه ذخیره‌سازی خود دوباره به دست می‌آورد و AD را به ثبت‌کننده شناسانه‌ی دارای تخلص (PIR) منقل می‌کند که *PI بر اساس نمونه کاوشگر زیست‌سنجشی اخذشده تولید می‌کند. *PI نتیجه شده با PI با کارخواه ذخیره‌شده است مقایسه می‌شود و نتیجه مقایسه با زیرسامانه تصمیم‌گیری ارتباط برقرار می‌کند تا یک خروجی درستی سنجی تولید شود.



شکل ۱۹- الگوی H: ذخیره توزیع شده در نمودافزار و کارخواه و مقایسه در کارخواه

در این الگو کارخواه می‌تواند یک نوع باجه باشد، همان‌طور که در مکان‌های عمومی پیدا می‌شود مثل فرودگاه‌ها و در ساختمان‌های عمومی برای اصالت‌سنجی شخصی. همچنین این الگو می‌تواند در تنظیمات واپایش مرز با استفاده از گذرنامه الکترونیکی (یا نمودافزار دیگر) در یک برنامه کاربردی مسافر ثبت‌نام‌شده به کار رود.

اصطلاحات زیر می‌تواند برای این الگو به کار گرفته شود:

- ذخیره IR در کارخواه به جای نمودافزار
- ذخیره PI در نمودافزار و AD در کارخواه

همان‌طور که در این بند توضیح داده شد، بیشتر سامانه‌های زیست‌سنجشی در بیشتر اوقات شامل یک کارساز و چند کارخواه متصل به‌طور خودکار است که با افزاره‌های اخذ زیست‌سنجشی مجهز شده‌اند. به‌طورکلی، میانگین سطح امنیت فرایند اصالت‌سنجی زیست‌سنجشی هم‌بستگی به سطح امنیت فرایند اجرا شده و هم‌بستگی به سطح عملکرد کارکردی افزاره‌های زیست‌سنجشی اخذشده دارد. با به دست آوردن اطلاعات مورد اعتماد مثل سطح عملکرد کارکردی افزاره زیست‌سنجشی استفاده‌شده و سطح امنیت سامانه خودکار، درستی‌سنج اصالت‌سنجی می‌تواند تصمیم بهتری در مورد وسعت بگیرد که نتیجه درستی سنجی

زیست‌سنجشی بتواند مورد اعتماد باشد. برای این مورد، زمینه‌ی اصالت‌سنجی برای زیست‌سنجه[1] (ACBio) که در استاندارد ISO /IEC 24761 معرفی شده‌اند می‌توانند به عنوان راه‌حلی برای مورد بالا به‌وسیله فرستادن اطلاعات راجع به افزاره‌های استفاده‌شده و فرایند اجرا شده در یک بخش خودکار به درستی سنجی به کار رود.

1 - Authentication Context for Biometrics

پیوست الف

(آگاهی‌دهنده)

پیوند و استفاده امن از DB_{IR} و DB_{BR} جداشده

الف-۱ عمومی

حتی اگر دو DB برای جداسازی داده زیست‌سنجشی استفاده شوند تا تاثیر تجاوز حریم خصوصی را کمینه کنند، توصیه می‌شود برای کاربرد آن‌ها، با یک شناسانه عام CI محدود باشند. به هر حال توصیه می‌شود یکی از آن‌ها هیچ‌گاه قادر نباشد اطلاعاتی راجع به داده از CI استخراج کند. اگر یک DB مورد تجاوز قرار گیرد و محتوی آن نقض شود، توصیه می‌شود عملگرهای دو DB قادر به آشکار کردن آن باشند. به‌طور مشابه اگر در طی استفاده از DB ها یک عملگر قانونی DB با کلید صحیح محتوای خود را اصلاح کند، توصیه می‌شود DB دیگر قادر به آشکارسازی اصلاحیه باشد.

در این پیوست مثال‌ها برای پیوند امن یک جفت IR و BR که فرض می‌شود دادگان جداشده برای IR و BR هستند با واپایش جدا شده و کاربرد آن‌ها توضیح داده خواهد شد. دادگان برای مرجع شناسه DB_{IR} و برای مرجع زیست‌سنجشی DB_{BR} نامیده خواهد شد. فرض می‌شود که DB_{IR} از یک کلید محرمانه K_i و DB_{BR} از یک کلید محرمانه K_b برای حفاظت از محتوای دادگان‌شان استفاده می‌کنند. به‌علاوه فرض می‌شود که دادگان ۲ کلید محرمانه را به اشتراک می‌گذارند: K_{ib} برای محاسبه کردن CI و یک بررسی رمزگذاری و K_e برای امن کردن پیام‌های اطلاعاتی (اگر لازم باشد).

الف-۲ پیوند امن بین DB_{IR} و DB_{BR} جدا شده

کانال ارتباطی بین DB_{IR} و DB_{BR} هم امن و هم ناامن است، باوجود یک کانال امن که محرمانگی و اصالت را تامین می‌کند. در مورد اول (مورد A)، فرض می‌شود کانال ارتباطی بین دو دادگان امن باشد. در مورد دوم (مورد B) فرض می‌شود کانال ارتباطی ناامن باشد، ولی دو دادگان یک رمز متقارن و یک کلید محرمانه K_e را به اشتراک می‌گذارند. پیوند امن بین مجموعه خالص IR و BR در زیر شرح داده شده است:

مورد A: کانال ارتباطاتی امن بین DB_{IR} و DB_{BR}

الف) دادگان مرجع شناسه DB_{IR} یک IR معتبر از یک IR مدعی (شخص) یا از یک TTP دریافت می‌کند، IR را با استفاده از K_i رمزگذاری می‌کند تا $EK_i(IR)$ را بگیرد و IR را درهم‌سازی[1] کند تا h(IR) را بگیرد.

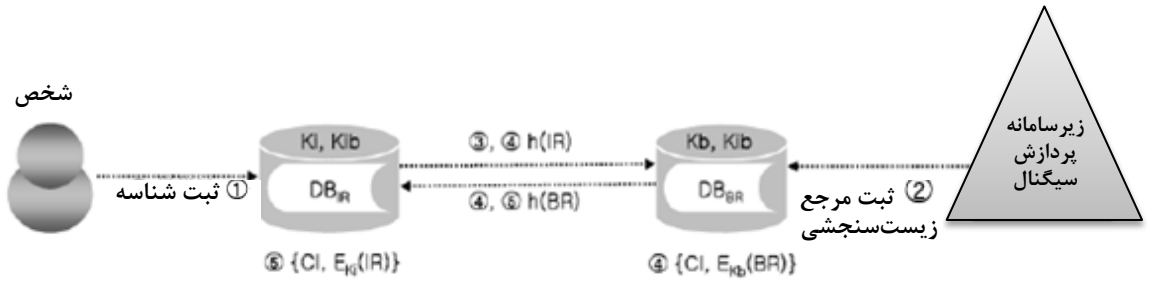
ب) دادگان مرجع شناسه DB_{IR}، BR متناظر را از یک زیرسامانه پردازش سیگنال دریافت می‌کند، BR را با استفاده از K_b رمزگذاری می‌کند تا $EK_b(BR)$ را بگیرد و BR را درهم‌سازی می‌کند تا h(BR) را بگیرد.

1 - Hash

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

ت) دادگان مرجع شناسه DB_{IR}، h(IR) را از DB_{IR} دریافت می‌کند، MAC را برای {h(IR),h(BR)} با کلید محرمانه K_{ib} اشتراک گذاشته شده محاسبه می‌کند تا $CI=MAC_{Kib}(h(IR),h(BR))$ را به دست آورد. CI به عنوان شناسانه عام ارزش بررسی رمزگذاری استفاده خواهد شد، h(BR) را به DB_{IR} می‌فرستد و {CI, $EK_i(IR)$} را ذخیره می‌سازد.

ث) دادگان مرجع شناسه DB_{IR}، h(BR) را از DB_{BR} دریافت می‌کند، MAC را برای {h(IR),h(BR)} با کلید محرمانه K_{ib} اشتراک گذاشته شده محاسبه می‌کند تا $CI=MAC_{Kib}(h(IR),h(BR))$ را به دست آورد، و {CI, $EK_i(IR)$} را ذخیره می‌سازد.



شکل الف-۱- پیوند امن بین DB_{IR} و DB_{BR} جدا شده (مورد A)

مورد B: کانال ارتباطاتی ناامن بین DB_{IR} **و** DB_{BR} با کلید محرمانه K_e مشترک شده

الف) دادگان مرجع شناسه DB_{IR} یک IR معتبر از یک IR مدعی (شخص) یا از یک TTP دریافت می‌کند، IR را با استفاده از K_i رمزگذاری می‌کند تا $EK_i(IR)$ را بگیرد و IR را درهم‌سازی کند تا h(IR) را بگیرد و با استفاده از K_e می‌تواند {h(IR), $IDDB_{IR},N_i$} را رمزگذاری کند تا EK_e{h(IR), $IDDB_{IR},N_i$} را بگیرد. IDDB یک شناسه منحصر به فرد برای DB و N_i فعلاً یک (مهر زمان یا عدد ترتیبی) است که توسط DB_{IR} تولید می‌شود.

ب) دادگان مرجع شناسه DB_{IR}، BR متناظر را از یک زیرسامانه پردازش سیگنال دریافت می‌کند، BR را با استفاده از K_b رمزگذاری می‌کند تا $EK_b(IR)$ را بگیرد و BR را درهم‌سازی می‌کند تا h(BR) را بگیرد.

پ) دادگان مرجع شناسه DB_{IR}، EK_e{h(IR), $IDDB_{IR},N_i$} را به DB_{BR} می‌فرستد.

ت) دادگان مرجع شناسه DB_{IR}، EK_e{h(IR), $IDDB_{IR},N_i$} را از DB_{IR} دریافت می‌کند، آن را برای بازیافتن {h(IR), $IDDB_{IR},N_i$} آشکار می‌سازد، و $IDDB_{IR}$ و N_i را بررسی می‌کند (اگر بررسی موفق نشد، با یک پیام خطا متوقف می‌شود). DB_{BR}، MAC را برای {h(IR),h(BR)} با کلید محرمانه K_{ib}

اشتراک گذاشته شده محاسبه می‌کند تا ($CI=MAC_{Kib}(h(IR),h(BR))$ را به دست آورد. CI بـه عنـوان شناسانه عام و به‌عنوان ارزش بررسی استفاده خواهد شد. $\{CI, h(BR), IDDB_{BR},N_b\}$ را با استفاده از K_e رمزگذاری می‌کند تـا $EK_e\{CI, h(BR), IDDB_{BR},N_b\}$ را بگیـرد و آن را بـه DB_{IR} مـی‌فرسـتد و $\{CI,$ $EK_b(BR)\}$ را ذخیره می‌سازد.

ث) دادگان مرجع شناسه DB_{IR}، $EK_e\{CI, h(BR), IDDB_{BR},N_b\}$ را از DB_{BR} دریافـت مـی‌کنـد، آن را برای بازیافتن $\{CI, h(IR)\}$ آشکار می‌سازد، و $IDDB_{BR}$ و N_b را بررسی می‌کند (اگر بررسی موفق نشد، با یک پیام خطا متوقف می‌شود). DB_{IR}، MAC را بـرای $\{h(IR),h(BR)\}$ بـا کلیـد محرمانـه K_{ib} اشـتراک گذاشته شده محاسبه می‌کند تا $(CI=MAC_{Kib}(h(IR),h(BR))$ را بـه دسـت آورد. آن را بـا CI دریافـت شده مقایسه می‌کند (اگر مقایسه موفق نشد، با یـک پیـام خطـا متوقـف مـی‌شـود) و $\{CI, EK_i(IR)\}$ را ذخیره می‌سازد.

الف-۳ ادعای BR برای درستی سنجی

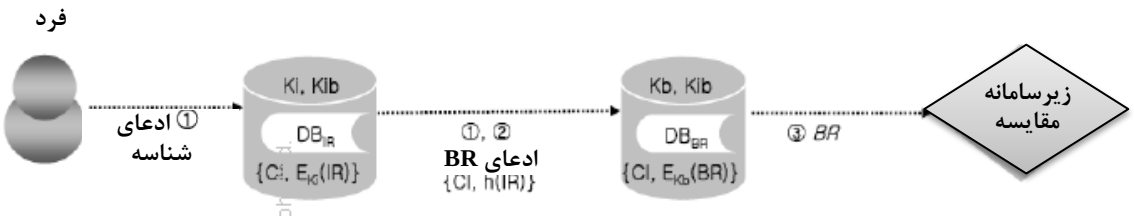
در این زیر بند، یک مثال از یک BR ادعا شده از DB_{IR} به DB_{BR} برای درستی سنجی شرح داده خواهد شد. در اینجا فرض می‌شود روش برای پیدا کردن $EK_i(IR)$ صحیح از یک شناسه قانونی ادعا داده شده است.

مورد A: کانال ارتباطاتی امن بین DB_{IR} **و** DB_{BR}

الف) به‌محض دریافت یک شناسه قانونی ادعاشده از یک مدعی IR (شخص) یـا یـک TTP، DB_{IR}، $EK_i(IR)$ متناظر را آشکار می‌کند تا IR دریافت و آن را برای گرفتن h(IR) درهم‌سازی می‌کنـد و $\{CI, h(IR)\}$ را بـه DB_{BR} می‌فرستد.

ب) دادگان مرجع زیسـت‌سنجشـی DB_{BR}، $\{CI, h(IR)\}$ را از DB_{IR} دریافـت مـی‌کنـد، بـا اسـتفاده از CI، $EK_b(BR)$ را برای گرفتن BR آشکار می‌سازد. BR را برای گرفتن h(BR) درهم‌سازی مـی‌کنـد، MAC_{Kib} $(h(IR),h(BR))$ را محاسبه می‌کند و با CI دریافت شده مقایسه می‌نماید.

پ) اگر آن‌ها مطابق بودند، DB_{BR}، BR را به‌طور امن به زیرسامانه مقایسه می‌فرستد. اگر تطابق موفق نبـود، با یک پیام خطا متوقف می‌شود.



شکل الف-۲- ادعای BR برای درستی سنجی (مورد A)

مورد B: کانال ارتباطاتی ناامن بین DB_{IR} **و** DB_{BR} با کلید محرمانه K_{ib} مشترک شده

الف) به‌محض دریافت یک شناسه قانونی ادعا از یک IR مدعی (شخص) یا یک TTP، DB_{IR}، $EK_i(IR)$ متناظر را آشکار می‌کند تا IR بگیرد و آن را برای گرفتن h(IR) درهم‌سازی می‌کند، {CI, h(IR), $IDDB_{IR},N_i$} را رمزگذاری می‌کند تا

EK_{ib}{CI, h(IR), $IDDB_{IR},N_i$} را بگیرد و آن را به DB_{BR} بفرستد.

ب) دادگان مرجع زیست‌سنجشی DB_{BR}، EK_{ib}{h(IR), $IDDB_{IR},N_i$} را از DB_{IR} دریافت می‌کند، آن را برای بازیافتن {CI, h(IR), $IDDB_{IR},N_i$} آشکار می‌سازد، و $IDDB_{IR}$ و N_i را بررسی می‌کند (اگر بررسی موفق نشد، با یک پیام خطا متوقف می‌شود). $EK_b(BR)$ را با استفاده از CI پیدا می‌کند، $EK_b(BR)$ را برای گرفتن BR آشکار می‌سازد. BR را برای گرفتن h(BR) مخلوط می‌کند،

MAC_{Kib} (h(IR),h(BR)) را محاسبه می‌کند و با CI دریافت شده مقایسه می‌نماید.

پ) اگر آن‌ها مطابق بودند، DB_{BR}، BR را به‌طور امن به زیرسامانه مقایسه می‌فرستد. اگر تطابق موفق نبود، با یک پیام خطا متوقف می‌شود.

الف-۴ ادعای IR برای شناسایی

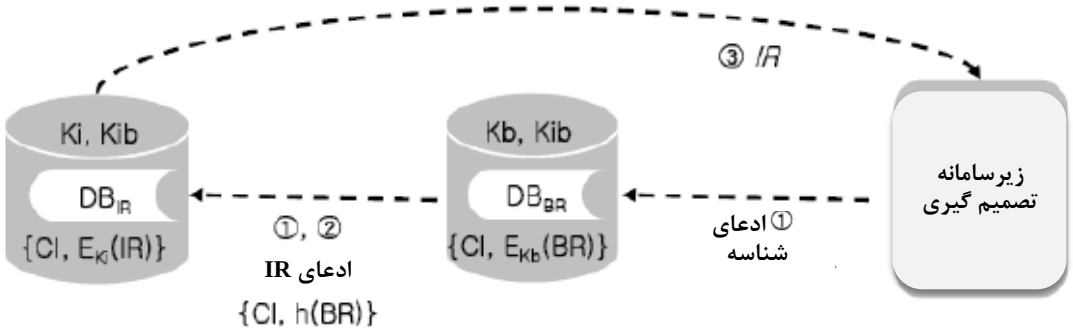
در این زیر بند، یک مثال از یک IR ادعا شده از DB_{BR} به DB_{IR} برای درستی سنجی شرح داده خواهد شد. در اینجا فرض می‌شود که DB_{BR}، $EK_b(BR)$ را برای گرفتن BR آشکار ساخته و ان را به زیرسامانه مقایسه فرستاده است.

مورد A: کانال ارتباطاتی امن بین DB_{IR} **و** DB_{BR}

الف) به‌محض دریافت یک شناسه قانونی درخواست شده از زیرسامانه تصمیم‌گیریDB_{BR}, BR را برای گرفتن h(BR) مخلوط می‌کند و {CI, h(BR)} را به DB_{IR} می‌فرستد.

ب) دادگان مرجع شناسه DB_{IR}، {CI, h(BR)} را از DB_{BR} دریافت می‌کند EKi(IR) را با استفاده از CI پیدا می‌کند، $EK_i(IR)$ را برای گرفتن IR آشکار می‌سازد. IR را برای گرفتن h(IR) مخلوط می‌کند، MAC $_{Kib}$ (h(IR),h(BR)) را محاسبه می‌کند و با CI دریافت شده مقایسه می‌نماید.

پ) اگر آن‌ها مطابق بودند، DB_{IR}، IR را به‌طور امن به زیرسامانه مقایسه می‌فرستد. اگر تطابق موفق نبود، با یک پیام خطا متوقف می‌شود.



شکل الف-۳- ادعا IR برای درستی سنجی (مورد A)

مورد B: کانال ارتباطاتی ناامن بین DB_{IR} و DB_{BR} با کلید محرمانه K_{ib} مشترک شده

الف) به‌محض دریافت یک شناسه قانونی درخواست شده از زیرسامانه تصمیم‌گیریDB_{BR}, BR را برای گرفتن h(BR) مخلوط می‌کند، {CI, h(BR), $IDDB_{BR}$,N_b} را رمزگذاری می‌کند تا EK_e{CI, h(BR), $IDDB_{BR}$,N_b} را بگیرد. N_b فعلا توسط DB_{BR} تولیدشده است. EK_e{CI, h(BR), $IDDB_{BR}$,N_b} را به DB_{IR} می‌فرستد.

ب) دادگان مرجع شناسه DB_{IR}، EK_e{CI, h(BR), $IDDB_{BR}$,N_b} را از DB_{BR} دریافت می‌کند. آن را برای بازیافتن {CI, h(BR), $IDDB_{BR}$,N_b} آشکار می‌سازد، و $IDDB_{BR}$ و N_i را بررسی می‌کند (اگر بررسی موفق نشد، با یک پیام خطا متوقف می‌شود). EK_i(IR) را با استفاده از CI پیدا می‌کند، EK_i(IR) را برای گرفتن IR آشکار می‌سازد. IR را برای گرفتن h(IR) مخلوط می‌کند،

MAC_{Kib} (h(IR),h(BR)) را محاسبه می‌کند و با CI دریافت شده مقایسه می‌نماید.

پ) اگر آن‌ها مطابق بودند، DB_{IR}، IR را به‌طور امن به زیرسامانه مقایسه می‌فرستد. اگر تطابق موفق نبود، با یک پیام خطا متوقف می‌شود.

پیوست ب

(آگاهی‌دهنده)

الگوریتم‌های رمزگذاری برای امنیت سامانه زیست‌سنجشی

ب-۱ الگوریتم‌های رمزگذاری محرمانگی را تامین می‌کنند

برای تامین محرمانگی داده، الگوریتم‌های رمزگذاری می‌توانند استفاده شوند. یک الگوریتم رمزگذاری برای داده به کار گرفته می‌شود (اغلب متن اصلی یا متن آشکار[1] نامیده می‌شوند) تا داده رمزگذاری‌شده (یا متن رمزی) حاصل دهد: این فرایند به عنوان رمزگذاری شناخته می‌شود. الگوریتم رمزگذاری به روشی طراحی شده است که متن رمزی هیچ اطلاعاتی در مورد متن ساده حاصل نمی‌دهد، به‌جز، طول آن. با هر الگوریتم رمزگذاری یک الگوریتم آشکارسازی متناظر همبسته است که متن رمزی را به متن ساده اصلی تبدیل می‌کند.

رمزها با همبستگی با یک کلید کار می‌کنند. در یک رمز متقارن، از یک کلید مشابه در الگوریتم‌های رمزگذاری و آشکارسازی استفاده می‌شود. استاندارد ISO /IEC 18033-3 و استاندارد ISO /IEC 18033-4 به دو دسته مختلف از رمزهای متقارن اختصاص یافته‌اند: رمزهای بلوکی[2] و رمزهای جریانی[3]. کلید استفاده‌شده در رمز متقارن منسوب به کلید محرمانه است. در یک رمز متقارن کلیدهای مربوط و مختلف برای رمزگذاری و آشکارسازی استفاده‌شده است. استاندارد ISO /IEC 18033-2 به رمزها غیرمتقارن اختصاص دارد. رمزها غیرمتقارن از یک کلید رمزگذاری عمومی و یک کلید آشکارسازی خصوصی استفاده می‌کند. برای رمزگذاری داده زیست‌سنجشی رمزها کلید متقارن اغلب بیشتر از رمزها غیرمتقارن استفاده می‌شوند.

ب-۲ الگوریتم‌های رمزگذاری یکپارچگی را تامین می‌کنند

برای تامین بی‌نقصی داده می‌توان از الگوریتم کد اصالت‌سنجی پیام (MAC) و یا از الگوریتم امضای رقمی استفاده کرد. الگوریتم‌های MAC می‌توانند به عنوان راه‌کار یکپارچگی داده برای درستی سنجی اینکه داده در یک حالت غیرمجاز تغییر داده نشده استفاده شوند. همچنین آن ها می‌توانند به عنوان راهکار پیام اصالت-سنجی برای تامین اطمینان از اینکه پیام از یک نهاد دارای کلید محرمانه سرچشمه می‌گیرد استفاده شود. دو نوع MAC وجود دارد: راهکارهایی که از رمزهای بلوکی (به استاندارد ISO /IEC 9797-1 مراجعه شود) استفاده می‌کنند و راهکارهایی که از یک تابع مختلط اختصاص یافته (به استاندارد ISO /IEC 9797-2 مراجعه شود) استفاده می‌کنند.

---

1 - Cleartext
2 - Block ciphers
3 - Stream ciphers

امضای رقمی می‌تواند به جای امضای کتبی برای پیاده‌سازی خدمات مثل نهاد و اصالت‌سنجی پیام استفاده شود. آن ها همچنین می‌توانند برای تامین یکپارچگی و انکارناپذیری پیام استفاده گردند. این خدمات برای پیام‌های رقمی که رشته‌های بیت هستند به کار گرفته می‌شود (به عنوان مثال، تسلسل عناصر یا اهداف داده).

بیشتر طرح‌واره‌های امضای رقمی بر اساس سامانه کلید عمومی هستند. این سامانه شامل یک فرایند است که جفت‌هایی از کلید تولید می‌کند (مثل یک کلید خصوصی و یک کلید عمومی)، یک فرایند از کلید خصوصی استفاده می‌کند و یک فرایند از کلید عمومی. نوع طرح‌واره امضای رقمی وجود دارد. وقتی تمام پیام یا قسمتی از آن می‌تواند از امضا بازیابی شود، طرح‌واره یک « طرح‌واره امضای رقمی که بازیابی پیام می‌دهد» نامیده می‌شود (به استاندارد ISO /IEC 9796 مراجعه شود). وقتی تمام پیام باید ذخیره و به همراه امضا فرستاده شود، طرح‌واره به نام « طرح‌واره امضای رقمی (امضای دیجیتال) با پیوست[1]» نامیده می‌شود (به استاندارد ISO /IEC 14888 مراجعه شود).

ب-۳ الگوریتم‌های رمزگذاری محرمانگی و یکپارچگی را تامین می‌کنند

برای تامین محرمانگی و یکپارچگی هم رمزگذاری و هم MAC یا امضا می‌توانند استفاده شوند. در حالی که این عملکردها می‌توانند به روش‌های زیادی ترکیب شوند، تمام ترکیبات این چنین راهکاری نمی‌توانند ضمانت امنیت مشابهی را تامین کنند. به عنوان نتیجه، مطلوب است که جزئیات دقیق اینکه چگونه توصیه می‌شود راهکارهای محرمانگی و یکپارچگی ترکیب شوند تا سطح بهینه‌ای از امنیت تامین شود، شرح شده شود. به‌علاوه، در برخی موارد، از طریق تعریف یک روش پردازش داده با هدف تامین حفاظت محرمانگی و یکپارچگی، منفعت‌های کاراییِ برجسته‌ای می‌تواند به دست آید. در استاندارد ISO /IEC 19772 راهکارهای رمزگذاری معتبر تعریف‌شده‌اند. این‌ها روش‌های پردازش داده برای تامین حفاظت یکپارچگی و محرمانگی می‌باشند. آن ها نوعاً شامل هم یک ترکیب معین از محاسبه MAC و رمزگذاری داده و هم استفاده از یک الگوریتم رمزگذاری برای تامین محرمانگی و یکپارچگی باشد.

1 - Digital signature scheme with appendix

پیوست پ

(آگاهی‌دهنده)

چارچوب مراجع زیست‌سنجشی تجدیدپذیر

پ-۱ مراجع زیست‌سنجشی تجدیدپذیر

مراجع زیست‌سنجشی تجدیدپذیر (RBR ها) شناسه‌های ابطال‌پذیر و یا تجدیدپذیری هستند که یک فرد یا موضوع داده را در یک حوزه معین به‌وسیله شناسه یگانه محافظت شده و بازسازی شده از یک نمونه زیست-سنجشی اخذشده ارائه می‌دهند. یک مرجع زیست‌سنجشی تجدیدپذیر اجازه دسترسی به داده اندازه‌گیری زیست‌سنجشی اصلی، قالب زیست‌سنجشی و یا شناسه واقعی صاحبش را نمی‌دهد. به‌علاوه یک مرجع زیست‌سنجشی تجدیدپذیر در خارج از حوزه خدمت معنایی ندارد.

مراجع زیست‌سنجشی تجدیدپذیر از چهار مرحله مجزا تبعیت می‌کنند:

الف) ایجاد RBR جدید از داده زیست‌سنجشی در طی مرحله ثبت

ب) استفاده عملکردی از RBR به عنوان مرجع برای درستی سنجی یک شناسه ادعا شده.

پ) انقضای اعتبار RBR و

ت) تجدید یا باطل شدن یک RBR اگر اعتبارش منقضی شده باشد یا RBR نقض شده باشد.

پ-۲ ایجاد

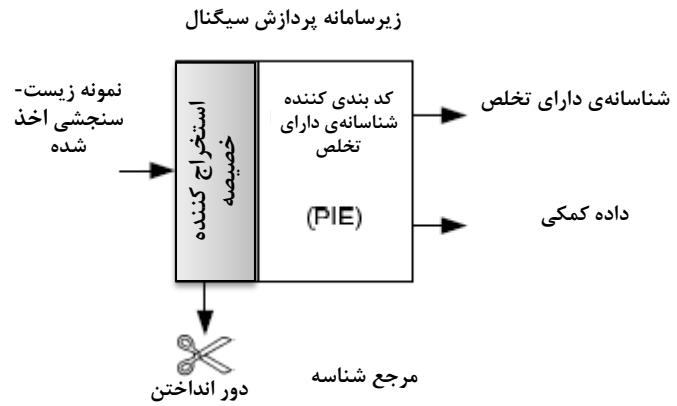
زیرسامانه پردازش سیگنال برای فرایند ایجاد RBR در شکل پ-۱ نشان داده شده است. یک پیکان در شکل جریان اطلاعات را ارائه می‌دهد. عموماً یک پروتکل را بین دو مرحله که به‌وسیله منبع یا مقصد پیکان بنیان نهاده شدند، ارائه می‌کند. مرحله استخراج خصیصه، داده خصیصه زیست‌سنجشی از نمونه زیست‌سنجشی اخذشده تولید می‌کند. خصیصه به‌طور ترجیح داده‌ای مطابق با استانداردهای موجود برای داده مرجع زیست‌سنجشی تولید می‌شوند که در استاندارد ISO /IEC 19794-X شرح داده شده است. متعاقباً یک کدبند شناسانه‌ی دارای تخلص (PIE) یک مرجع زیست‌سنجشی تجدیدپذیر تولید می‌کند که شامل شناسانه‌ی دارای تخلص و داده کمکی (AD) است. هرگاه RBR تولید شود، نمونه زیست‌سنجشی اخذشده و خصیصه‌های استخراج‌شده می‌توانند دور انداخته شوند.

داده کمکی می‌تواند یکی از اهداف زیر را به خدمت می‌گیرد:

- اجازه دوباره ایجاد کردن شناسانه‌ی دارای تخلص مرتبط با نمونه زیست‌سنجشی اخذشده برای مقایسه با شناسانه‌ی دارای تخلص مرجع
- اجازه تولید شناسانه‌های دارای تخلص مستقل و چندگانه از یک فرد در یک برنامه کاربردی برای

تامین مراجع تجدیدپذیر.

- اجازه تولید شناسانه‌ی دارای تخلص مستقل در میان برنامه‌های کاربردی برای جلوگیری از مقایسه و پیوند دادگان.
- تامین یک وسیله برای جداسازی داده مرجع زیست‌سنجشی (AD و PI) به منظور بالا بردن امنیت و حریم خصوصی و
- اجازه شخصی‌سازی پارامترهای مقایسه برای بهینه کردن عملکرد درستی سنجی.



شکل پ-۱– زیرسامانه پردازش سیگنال برای تولید مراجع زیست‌سنجشی تجدیدپذیر

داده کمکی (AD) می‌تواند از رویکردهای متفاوتی نتیجه شود که مراجع زیست‌سنجشی تجدیدپذیر تامین می‌کنند (برای مرور کلی به پیوست ت مراجعه شود). هم PI و هم AD ذخیره‌شده‌اند (یا با هم به عنوان ثبت دادگان و یا در ذخیره‌سازی جداگانه دادگان / رسانه‌ها ترکیب شده‌اند)، در حالی که تمام داده‌های زیست-سنجشی اخذشده دیگر به‌طور امن امحا شده‌اند. ترکیب PI و AD مرجع زیست‌سنجشی تجدیدپذیر (RBR) را شکل می‌دهد.

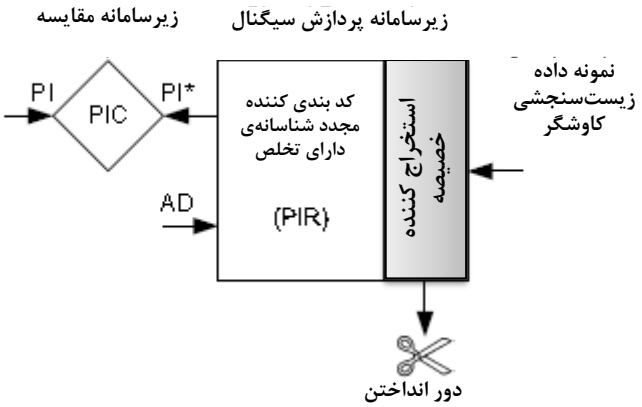
پ-۳ مقایسه

در یک فرانامه مقایسه خودکار، زیرسامانه‌های اخذ داده و پردازش سیگنال در یک طرف و زیرسامانه مقایسه در طرف دیگر به‌طور فیزیکی جدا شده‌اند (شکل پ-۲).

درستی سنجی نیاز به مراحل زیر دارد:

- مرحله استخراج خصیصه که نمونه داده زیست‌سنجشی کاوشگر را پردازش می‌کند.
- یک کدبند شناسانه‌ی دارای تخلص (PIR) که شناسانه‌ی دارای تخلص جدید (PI^*) را بر اساس داده کمکی تامین شده و خصیصه‌های استخراج‌شده تولید می‌کند.

- یک زیرسامانه مقایسه به‌وسیله مقایسه کننده شناسانه‌ی دارای تخلص (PIC)، PI را با PI^* مقایسه و یک امتیاز مقایسه تولید می‌کند.
- یک زیرسامانه تصمیم‌گیری (در شکل پ-۲ نشان داده نشده است) یک خروجی درستی سنجی بر اساس امتیاز مقایسه تامین می‌کند.



شکل پ-۲- زیرسامانه پردازش سیگنال و زیرسامانه مقایسه

پ-۴ منقضی شدن

مراجع زیست‌سنجشی تجدیدپذیر برای دلایل متعددی منقضی می‌شوند. به عنوان مثال، ممکن است یک RBR فقط برای دوره زمانی محدود انتشار یابد یا ممکن است تجدید شدن الزامی باشد زیرا نقض شده است.

به‌علاوه ممکن است تاثیرات کهنه شدن روی مشخصه زیست‌سنجشی اثر گذارد، که موردی برای چهره انسان است که نیاز به تجدید مرجع زیست‌سنجشی دارد. بررسی‌های اعتبار و منقضی شدن‌ها می‌توانند به‌وسیله فهرست‌های ابطال‌پذیری واپایش شوند.

پ-۵ ابطال

مرجع زیست‌سنجشی تجدیدپذیر (RBR) بسته به پیاده‌سازی سامانه درستی سنجی می‌توانند به‌وسیله موارد زیر باطل شوند:

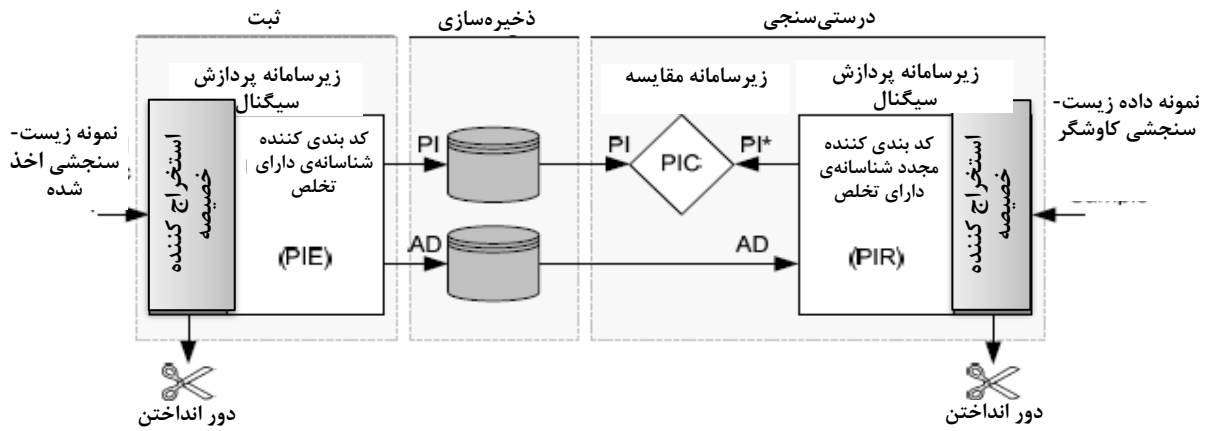
- حذف RBR از دادگان و / یا
- حذف اختیار استفاده از RBR

بعد از عمل ابطال، ثبت‌نام دوباره می‌تواند منجر به مرجع زیست‌سنجشی تجدید شده شود. بسته به پیاده‌سازی به کار گرفته شده، این ممکن است نیاز به اخذ نمونه‌های زیست‌سنجشی اصلی داشته باشد. در سایر پیاده‌سازی‌ها، ثبت دوباره بر اساس داده زیست‌سنجشی خام یا RBR های یدکی است که در دادگان با امنیت بالا ذخیره‌شده‌اند که هم به‌طور فیزیکی و هم منطقی از دادگان RBR عملکردی جدا شده‌اند تا اجازه

ثبت دوباره بدون حضور فیزیکی موضوع داده را بدهد.

پ-۶ مرورکلی معماری

فرایند ثبت، ذخیره‌سازی و درستی سنجی در شکل پ-۳ تعیین‌شده‌اند. زیرسامانه تصمیم‌گیری که به زیرسامانه مقایسه متصل است در شکل نشان داده نشده است.



شکل پ-۳- معماری برای مراجع زیست‌سنجشی تجدیدپذیر

پیوست ت

(آگاهی‌دهنده)

مثال‌های فناوری برای مراجع زیست‌سنجشی تجدیدپذیر

ت-۱ مرور کلی

روش‌های متنوع برای نتیجه گرفتن مراجع زیست‌سنجشی تجدیدپذیر انتشار یافته‌اند (برای اطلاعات پس‌زمینه به [۳۳] و [۲۴] مراجعه شود). جدول ت-۱ یک فهرست از مثال‌هایی تامین می‌کند که شامل مراجع و نگاشت بین عناصر داده متنوع از روش و عناصر داده معین شده در این استاندارد است.

جدول ت-۱- مرور کلی روش‌های تولید مراجع زیست‌سنجشی تجدیدپذیر

روش	مرجع	شناسانه‌ی دارای تخلص(PI)	داده کمکی(AD)
سامانه‌های داده کمک‌کننده	[22]	چکیده‌ی رشته محرمانه	داده کمک‌کننده
جهش فازی	[23]	چکیده‌ی رشته محرمانه	انحراف
رمزگذاری زیست‌سنجشی	[24]	کلید رمزگذاری	پالایه و کلید پیوند
تعهد فازی	[25]	چکیده‌ی رشته محرمانه	مجموعه نقطه P
توابع استحفاظ	[26]	چکیده‌ی رشته محرمانه	چالش اصالت‌سنجی W
استخراج کننده‌های فازی	[27]	چکیده‌ی رشته محرمانه	رشته عمومی P
PIR گسترده	[28]	قالب رمزگذاری‌شده	n/a
مدوله‌سازی نمایه کوانتش شش‌گوش ۲ بعدی[a]	[29]	چکیده‌ی رشته محرمانه	خطاهای کوانتش
زیست‌سنجه‌های ابطال‌پذیر	[31]	قالب تبدیل شده	پارامترهای تبدیل
چکیده‌ی مستحکم زیست-سنجشی	[36]	چکیده‌ی رشته دودویی مستحکم	تبدیل یک-طرفه
زیست-چکیده‌سازی	[37]	رشته دودویی مستحکم	ماتریس انعکاس تصادفی
کلید رمزگذاری با عمر کوتاه	[38]	کلیدهای رمزگذاری	پارامترهای سامانه

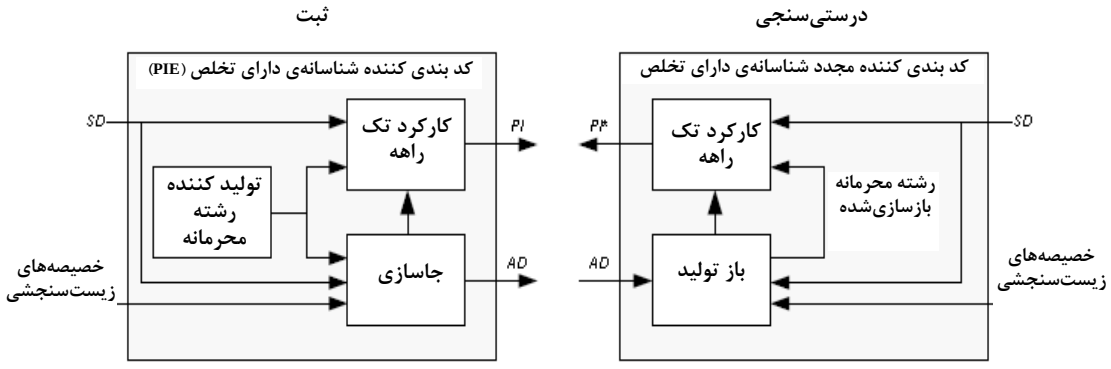
روش	مرجع	شناسانه‌ی دارای تخلص(PI)	داده کمکی(AD)
زیست نمودافزارها	[39]	جزییات رمزگذاری‌شده	کلیدهای رمزگذاری
طرح امن	[40]	باقیمانده کوانتش	کوانتش‌گر[b]
چکیده‌ی جزییات مستحکم	[41]	رشته دودویی مستحکم برای هر جزییات	جدول تنوع‌بخشی تصادفی

[a] 2D hexagonal quantization index modulation

[b] Quantizer

یک روش خیلی معمولی در شکل ت-۱ مجسم شده است. در طی ثبت کدبند شناسانه‌ی دارای تخلص به عنوان خصیصه‌های زیست‌سنجشی ورودی دریافت می‌شود. یک رشته محرمانه به‌وسیله تولیدکننده رشته محرمانه تولید می‌شود. متعاقباً، یک کارکرد (جاسازی) داده کمکی تولید می‌کند (همچنین منسوب به «طرح عمومی» است) که به‌وسیله ترکیب خصیصه‌های زیست‌سنجشی و رشته محرمانه انجام می‌گیرد.

در خیلی از پیاده‌سازی‌های تمرینی کارکرد، جاسازی برخی اشکال تدریج را شامل می‌شود (به عنوان مثال تبدیل داده خصیصه پیوسته برای رشته‌های تک گانه). شناسانه‌ی دارای تخلص با استفاده از کارکرد تک راهه رمزگذاری و رشته محرمانه به عنوان ورودی و داده کمکی انتخابی ایجاد می‌شود.



شکل ت-۱-پیاده‌سازی سطح بالا برای تولید مراجع زیست‌سنجشی تجدیدپذیر

در طی درستی سنجی، کدبند کننده شناسانه‌ی دارای تخلص داده کمکی و خصیصه‌های زیست‌سنجشی را به عنوان ورودی دریافت می‌کند. یک کارکرد دوباره تولید، رشته محرمانه را بر اساس خصیصه‌های زیست-سنجشی و داده کمکی دوباره تولید می‌کند. متعاقباً، یک شناسانه‌ی دارای تخلص (PI*) با استفاده از کارکرد

تک راهه با رشته محرمانه بازسازی شده تولید می‌شود.

پیاده‌سازی‌های متناوب می‌توانند از یک کاربر یا سامانه که ورودی اضافی تولید می‌کند (داده تکمیلی یا SD) استفاده کند تا خصیصه‌های زیست‌سنجشی را به عنوان بخشی از مرحله جاسازی یا به عنوان ورودی اضافی به کارکرد تک راهه به‌صورت تصادفی درآورد. این ورودی می‌تواند به عنوان مثال یک کلمه عبور محرمانه، کلید یا PIN را مقایسه کند. به‌طور متناوب، اگر فرض شود رشته تصادفی، عمومی و وابسته به موضوع باشد، این رشته می‌تواند بخشی از AD باشد.

کارکردهای جاسازی و تک راهه موضوع التزامات متنوعی برای حفاظت حریم خصوصی هستند. این الزامات شامل موارد زیر می‌باشند:

- آنتروپی مناسب در رشته‌های محرمانه تولیدشده. این الزام برای مجاز کردن تعداد تنوع‌بخشی‌های RBR ها برای یک فرد نیاز است.
- بازگشت‌ناپذیری کدبند شناسانه‌ی دارای تخلص که کارکردی تولید می‌کند تا از بازسازی زیست-سنجشی یا رشته محرمانه از PI جلوگیری کند.
- پیوند ناپذیری RBR ها که برای کاربردهای متفاوت با استفاده از خصیصه‌های زیست‌سنجشی مساوی تولیدشده است تا از تطابق دادگان جلوگیری کند.

پیوست ث

(آگاهی‌دهنده)

ته‌نقش‌گذاری[1] زیست‌سنجشی

ث-۱ ته‌نقش‌گذاری زیست‌سنجشی

ته‌نقش‌گذاری زیست‌سنجشی یک روش حفاظت نمونه زیست‌سنجشی است که از اطلاعات مناسب در مورد سازمان، دوره زمانی اعتبار و شناسه‌های منحصر به فرد نمونه زیست‌سنجشی به عنوان یک ته‌نقش‌گذار استفاده می‌کند تا از توزیع‌های غیرقانونی و سوء استفاده از نمونه زیست‌سنجشی جلوگیری کند.
ته‌نقش‌گذاری همچنین می‌تواند انکارناپذیری و پیگردی خصیصه‌ها را تامین کند تا از توزیع غیرقانونی نمونه‌های زیست‌سنجشی جلوگیری شود.

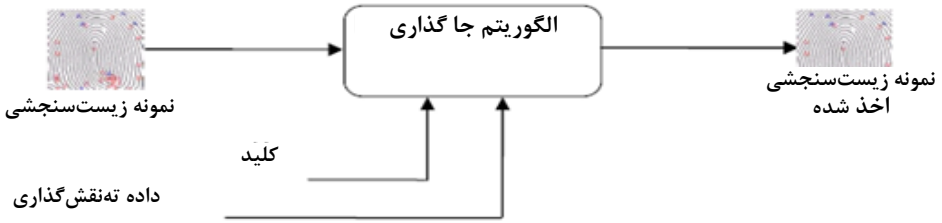
ته‌نقش‌گذاری زیست‌سنجشی شامل دو فرایند اصلی است:

- ایجاد و جاسازی ته‌نقش‌گذار زیست‌سنجشی
- استخراج ته‌نقش‌گذار جاسازی‌شده از نمونه زیست‌سنجشی ته‌نقش‌گذاری شده

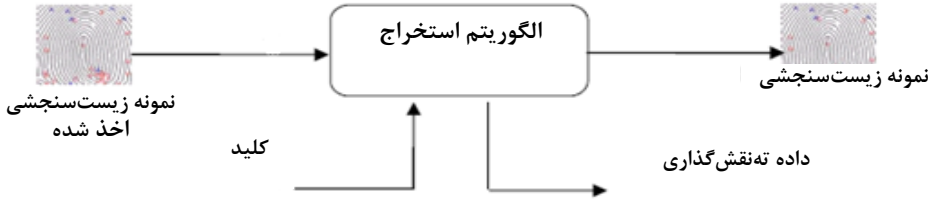
ث-۲ درج و استخراج یک ته‌نقش‌گذار زیست‌سنجشی

داده ته‌نقش‌گذار جاسازی‌شده حاوی اطلاعات مرتبط با نمونه زیست‌سنجشی به ته‌نقش‌گذار دوبعدی تبدیل شده است. ته‌نقش‌گذار در محدوده‌های مناسب بدون تحریف کردن نمونه زیست‌سنجشی به‌وسیله الگوریتم درج جاسازی‌شده است و سپس نمونه زیست‌سنجشی ته‌نقش‌گذاری شده سرانجام به دست می‌آید. فرایند استخراج می‌تواند به عنوان فرایند معکوس فرایند جاسازی توضیح داده شود که در شکل ث-۱ نشان داده شده است.

1 - Watermarking



الف) فرایند جاسازی در ته‌نقش‌گذاری زیست‌سنجشی



ب) فرایند استخراج در ته‌نقش‌گذاری زیست‌سنجشی

شکل ث-۱- فرایند ته‌نقش‌گذاری زیست‌سنجشی

ث-۳ مثال‌های کاربردی

- حفاظت از نمونه زیست‌سنجشی از استفاده غیرمجاز

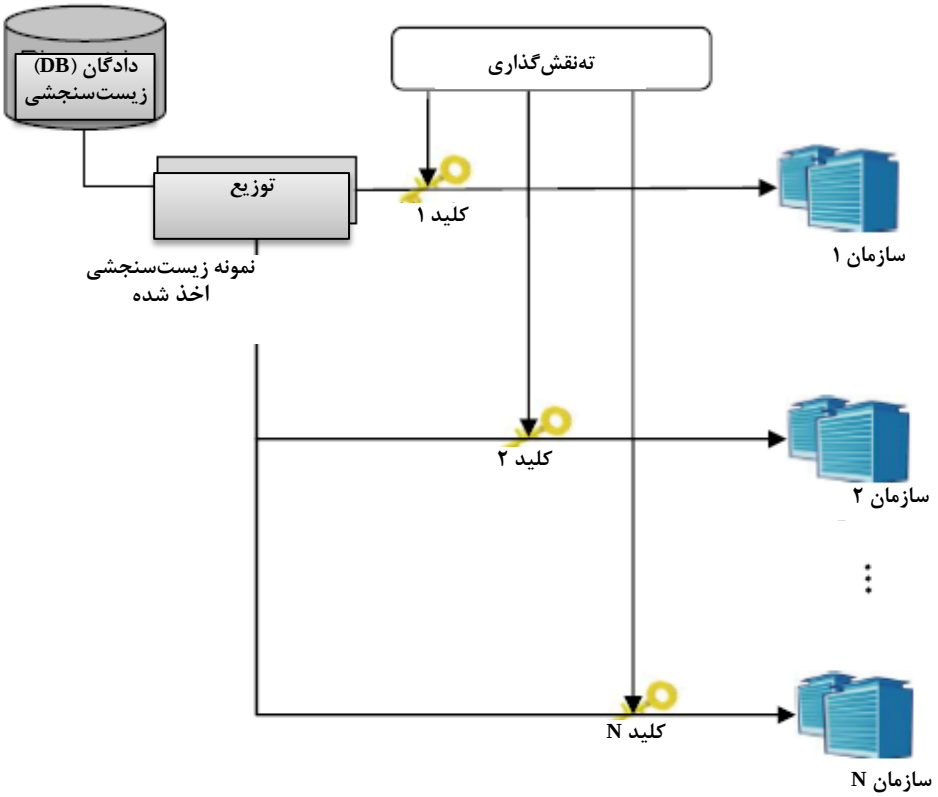
بعد از اخذ نمونه زیست‌سنجشی در طی فرایند ثبت، یک ته‌نقش‌گذار زیست‌سنجشی می‌تواند در نمونه زیست‌سنجشی جاسازی شود و سپس نمونه زیست‌سنجشی ته‌نقش‌گذاری شده می‌تواند در دادگان ثبت ذخیره شود. با آزمودن ته‌نقش‌گذار استخراج‌شده در لحظه بازیافتن نمونه زیست‌سنجشی از دادگان ثبت، ثبت اطلاعات زیست‌سنجشی غیرقانونی یا ته‌نقش‌گذار نامناسب دارد یا اصلاً ته‌نقش‌گذاری ندارد که بتواند به‌سرعت آشکار شود.

- شناسایی منبع توزیع نمونه‌های زیست‌سنجشی فاش شده

اگر اطلاعات مرتبط با شخص مسئول به عنوان ته‌نقش‌گذار زیست‌سنجشی در لحظه به دست آوردن نمونه زیست‌سنجشی جاسازی‌شده باشد، منبع توزیع نمونه‌های زیست‌سنجشی فاش شده می‌تواند یافت شود، هرگاه هرگونه فاش‌سازی غیرقانونی از نمونه زیست‌سنجشی اتفاق افتد.

- پیگردی سازمان‌های مسئول برای نمونه‌های زیست‌سنجشی فاش شده

داده زیست‌سنجشی می‌تواند در سازمان‌های متعددی مطابق با ضرورت‌های قضایی توزیع شود. به هر حال توزیع نمونه‌های زیست‌سنجشی احتمال فاش‌سازی‌های غیرقانونی را بالا می‌برد؛ بنابراین پیش از توزیع به هر سازمان، یک شناسه سازمانی منحصر به فرد می‌تواند به عنوان ته‌نقش‌گذار زیست‌سنجشی جاسازی شود که در شکل ث-۲ نشان داده شده است.



شکل ث-۲- پیگردی توزیع غیرقانونی با استفاده از ته‌نقش‌گذاری زیست‌سنجشی

در مواردی که N منبع توزیع وجود داشته باشد که هرکدام یک شناسه به عنوان ته‌نقش‌گذار زیست‌سنجشی دارند، اگر هرگونه شکی در مورد قانونی بودن نمونه زیست‌سنجشی وجود داشته باشد، منبع فاش‌سازی می‌تواند از ته‌نقش‌گذار استخراج‌شده شناسایی شود.

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 ciphers2*)

[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*

[۱۷] استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی - سیستم های (سامانه‌های) مدیریت امنیت اطلاعات-مرور کلی و واژگان

[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*

[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