الزامات به‌کارگیری فن‌آوری بیومتریک در ارتقاء امنیت اطلاعات با رویکرد پدافند غیرعامل

ذکریا کاظم‌پور[1]
اسماعیل شیرزادی[2]

تاریخ دریافت: ۱۳۹۴/۱۰/۲۰ تاریخ تأیید: ۱۳۹۴/۱۲/۱۵

چکیده

اطلاعات در سازمان‌ها، مؤسسه‌های پیشرفته و جوامع علمی، شاهرگ حیاتی محسوب می‌گردد. دست‌یابی به اطلاعات و عرضه مناسب و سریع آن، همواره مورد توجه سازمان‌هایی است که اطلاعات در آن‌ها دارای نقش محوری و سرنوشت‌ساز است.

از طرفی کنترل دست‌یابی و نحوه استفاده از این اطلاعات از چالش‌های مهم این عرصه است. در این راستا لازم است هر سازمان برای حفاظت از اطلاعات ارزشمند خود و تأمین امنیت آن به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی خود را پیاده‌سازی و اجرا نماید.

امروزه به‌علت اهمیت روز افزون اطلاعات و تمایل افراد و سازمان‌ها به امنیت بیشتر آن به‌ویژه در رایانه‌ها، ابزارهای قدیمی مانند استفاده از گذرواژه به‌تنهایی جواب‌گو و قابل اعتماد نیست. در این راستا متخصصان به‌دنبال راه‌هایی مطمئن‌تر هستند که یکی از موفق‌ترین راه‌های یافته شده، استفاده از علم و فن‌آوری‌های بیومتریک[3] است.

در این مقاله با توجه به هدف اصلی تحقیق، ضمن معرفی فن‌آوری بیومتریک و روش‌های معمول آن، نیازمندی به‌کارگیری این فن‌آوری برای ارتقای امنیت اطلاعات از منظر پدافند غیرعامل استخراج و مورد تأکید قرار گرفته است.

واژگان کلیدی: *اطلاعات، امنیت اطلاعات، بیومتریک، پدافند غیرعامل.*

---

۱. کارشناسی‌ارشد پدافند غیرعامل گرایش امنیت ملی دانشکده علوم و فنون فارابی، نویسنده مسئول، رایانامه؛ (z.kazempour@gmail.com).
۲.کارشناسی‌ارشدمخابرات سیستم‌ومدرس دانشکده علوم‌و فنون‌فارابی،رایانامه؛(mohammadshirzadi1383@gmail.com).

3. Biometrics Tecnology

مقدمه

فن‌آوری بیومتریک، امروز به‌عنوان یکی از فن‌آوری‌های پیشرفته در جهان، با توجه به کاربردهای بسیار زیاد و نیازمندی به‌وجود آمده برای استفاده از آن، به‌سرعت در حال پیمودن پله‌های رشد است. در این راستا تعداد محدودی از کشورهای جهان نقش عمده‌ای در این پیش‌برد داشته و وضعیت خود را از این بابت در جهان تثبیت کرده‌اند. فراگیر شدن استفاده از فن‌آوری بیومتریک در جهان و همچنین وجود برخی قوانین جهانی در این راستا، دیگر کشورها را نیز به‌سوی این فن‌آوری سوق داده است. یکی از دلایل مهم برای ورود به جمع صاحبان فن‌آوری بیومتریک و بومی‌سازی آن، وجود ویژگی‌های امنیتی در این فن‌آوری و اهمیت آن برای برخی از کشورها از جمله جمهوری اسلامی ایران است (فولادوند، ۱۳۸۹: ۱۹).

بیومتریک نمونه‌ای از فن‌آوری‌های نوظهور در دنیای ارتباطات و اطلاعات بوده که به قولی شاه‌کلید ورود به دنیای اطلاعات و کنترل ارتباطات است. در گزارش ژانویه سال ۲۰۰۰ دانشگاه ام‌آیتی، از بیومتریک به عنوان یکی از ده فن‌آوری جدید که دنیا را تغییر خواهد داد، نام برده شده است. اجرای پروژه‌های عظیم امنیت بیومتریکی در جهان نمایانگر اهمیت این فن‌آوری درارتباطات بین‌المللی آینده است.

فن‌آوری بیومتریک در زمینه تأمین امنیت و کنترل دسترسی فیزیکی و منطقی به منابع مالی، اطلاعاتی، شبکه رایانه‌های مراکز حساس و همچنین صدور مدارک شناسایی قابل‌اطمینان و کاربردی در راستای افزایش امنیت در کنار بهبود دقت، سرعت، سهولت و کاهش هزینه‌ها را دارد.

تعامل افراد با سامانه‌های گوناگون، در جوامع جدید، موجب پدید آمدن مفهوم جدیدی به نام هویت الکترونیکی (یا هویت سایبرنتیکی) شده است. تجلی این مفهوم در رواج استفاده از

مشخصه‌های بیومتریکی افراد برای شناسایی هویت آنها توسط سامانه‌های بیومتریکی در قالب پروژه‌های ملی و بین‌المللی کشورهای مختلف هویدا شده است (عابدی، ۱۳۸۸: ۶۳).

بیان مسئله

امروزه تنوع تهدیدها، ضرورت به‌کارگیری وسایل قابل‌اطمینان، سریع و غیرتهاجمی برای تشخیص هوشمند هویت اشخاص تعیین و تأیید دسترسی به اسناد و مدارک و ورود به اماکن حساس را به‌شکل قابل‌توجهی افزایش داده است که این امر سازمان‌های مختلف را نیازمند به استفاده از فن‌آوری‌ها و تجهیزات به‌روز نموده است.

در سازمان‌هایی هم که دارائی‌های ارزشمندی به‌نام اطلاعات را در اشکال مختلف آن نگهداری یا مبادله می‌نمایند، ضرورت به‌کارگیری ابزارها و روش‌هایی با قابلیت اطمینان بالا برای مدیریت امن اطلاعات و کنترل دسترسی‌ها بیش از پیش ضرورت پیدا کرده است. به‌همین منظور فن‌آوری بیومتریک با توجه به محاسن و قابلیت‌های منحصر به‌فرد خود و نیازمندی به‌وجود آمده، می‌تواند به‌عنوان یکی از ابزارهای قابل‌اتکا در این حوزه مورد بهره‌برداری قرار گیرد.

هدف این تحقیق، شناخت فن‌آوری بیومتریک و الزامات به‌کارگیری این فن‌آوری برای ارتقای امنیت اطلاعات.

پرسش اساسی نیز این است که از دیدگاه پدافند غیرعامل نیازمندی به‌کارگیری فن‌آوری بیومتریک در ارتقای امنیت اطلاعات کدامند؟

مبانی نظری تحقیق

برای ارائه یک تصویر روشن از موضوع تحقیق، ابتدا متغیرهای تحقیق تشریح و درنهایت ارتباط آن‌ها مورد بررسی و تحلیل توصیفی قرار خواهد گرفت.

پدافند غیرعامل[1]: این مفهوم دفاع را در ذهن متبادر می‌کند، یک مفهوم ذاتی است که از ابتدای خلقت تا به حال در زندگی بشر بوده و بشر همواره تلاش کرده تا به نوعی با اقدام‌های متفاوت و متنوع، بین تهدید و امنیت تعادل برقرار نماید. اغلب این تلاش‌ها در دو حوزه شکل می‌گیرد:

حوزه اول؛ تهدیدهای امنیتی و نظامی(تهدیدهای مصنوعی یا دست‌ساز بشر).

حوزه دوم؛ تهدیدهای طبیعی.

در حوزه اول ایجاد تعادل در برابر تهدیدها و اقدام‌های امنیتی و نظامی دشمنان و در حوزه دوم ایجاد تعادل در برابر تهدیدهای طبیعی، از رسالت‌های پدافند غیرعامل است.

توجه به تعاریف زیر به روشن‌تر شدن مفهوم پدافند غیرعامل کمک می‌نماید:

«پدافند غیرعامل» عبارت است از: به‌کارگیری هرگونه ابزار، شرایط و موقعیت، به‌طوری که خود به خود و بدون نیاز به عامل انسانی در مراحل مختلف، با تهدیدها و حمله‌های دشمن مقابله شود (نوروزی،۱۳۸۵:۵۶).

به‌عبارتی دیگر «پدافند غیرعامل» به تمامی اقدام‌ها و تدابیری گفته می‌شود که بدون استفاده از سلاح، موجب کاهش آسیب‌پذیری، تلفات و خسارات گردیده و موجب افزایش پایداری شود. «پدافند غیرعامل» عبارت است از: «به‌کار بردن روش‌هایی که از آثار زیان‌های ناشی از اقدام‌های دشمن بکاهد، یا آن‌را به حداقل برساند» (جلالی فراهانی، ۱۳۸۸:۸۰).

مجموعه اقدام‌های غیرمسلحانه‌ای که موجب کاهش آسیب‌پذیری نیروی انسانی، ساختمان‌ها و تأسیسات، تجهیزات و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن می‌گردد (آیین‌نامه اجرایی بند (۱۱) تبصره (۱۲۱) قانون برنامه پنج ساله چهارم توسعه کشور).

به‌دنبال سازمان یافتن ساختار اجرایی، سیاست‌گذاری و برنامه‌ریزی پدافند غیرعامل کشور در قالب کمیته دائمی و سازمان پدافند غیرعامل و نیز پی‌گیری اجرای برنامه‌ها، مفاهیم جدیدتری

1. Passive Defense

از پدافند غیرعامل مطرح گردیده که پس از آن، مجمع تشخیص مصلحت نظام کـه متشـکل از نمایندگان منتخب رهبر معظم انقلاب اسلامی به‌منظور تهیه پیش‌نویس سیاست‌های کلی نظام شکل گرفته است و با توجه به اهمیت مسئله، «پدافند غیرعامل» را با رویکرد جدید و با تعمیم پوشش و پاسخ‌گویی به تهدیدهای جدید اعم از حوزه نرم و سخت به شکل زیـر تعریـف نمـوده است. این مجموعه سیاست‌های کلی نظام را در حوزه پدافنـد غیرعامـل در قالـب سـیزده بنـد تعریف، تدوین و مصوب نمودند که دو مورد از ایـن بنـدها، سیاسـت‌گـذاری در حـوزه «امنیـت اطلاعات» و اقدام‌های مرتبط به این حوزه است که در ادامه مقاله به این مهم پرداختـه خواهـد شد.

تعریف جامع پدافند غیرعامل: «مجموعه اقدام‌های غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و آسانی در مدیریت بحران در مقابل تهدیدها و اقدام‌های نظامی دشمن می‌گردد».

امنیت اطلاعات[1]: از زمانی‌که نوشتن و تبادل اطلاعات آغاز شد، همه انسان‌ها به‌خصوص سران حکومت‌ها و فرماندهان نظامی در پی راه‌کاری برای محافظت از محرمانه بودن مکاتبات و تشخیص دست‌کاری آن‌ها بودند. ژولیوس سزار پنجاه سال قبل از میلاد یک سامانه رمزنگاری مکاتبه‌ای ابداع کرد تا از خوانده شدن پیام‌های سری خود به‌وسیله دشمن جلوگیری کند، حتی اگر آن پیام به‌دست دشمن بیفتد. جنگ جهانی دوم باعث پیشرفت چشم‌گیری در زمینه امنیت اطلاعات گردید و این آغاز کارهای حرفه‌ای در حوزه امنیت اطلاعات شد. پایان قرن بیستم و سال‌های اولیه قرن ۲۱ شاهد پیشرفت‌های سریع در ارتباط‌های راه‌دور، سخت‌افزار، نرم‌افزار و رمزگذاری داده‌ها بود. در دسترس بودن تجهیزات محاسبه‌ای کوچک‌تر، قوی‌تر و ارزان‌تر، پردازش الکترونیکی داده‌ها باعث شد که شرکت‌های کوچک و کاربران خانگی دسترسی

1. Information Security

بیشتری به آن‌ها داشته باشند. این تجهیزات به‌سرعت از طریق شبکه‌های رایانه مثل اینترنت به‌هم متصل شدند.

با رشد سریع و استفاده گسترده از پردازش الکترونیکی داده‌ها و کسب و کار الکترونیک از طریق اینترنت، همراه با ظهور بسیاری از خراب‌کاری‌های بین‌المللی، نیاز به روش‌های بهتر حفاظت از رایانه‌ها و اطلاعات آنها ملموس گردید. رشته‌های دانشگاهی از قبیل امنیت رایانه، امنیت اطلاعات و اطلاعات مطمئن همراه با سازمان‌های متعدد حرفه‌ای پدید آمدند. هدف مشترک این فعالیت‌ها و سازمان‌ها حصول اطمینان از امنیت و قابلیت اطمینان از سامانه‌های اطلاعاتی بوده است.

«امنیت اطلاعات» یعنی حفاظت اطلاعات و سامانه‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از: دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب کردن، تغییر، دست‌کاری.

«امنیت اطلاعات»، به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد.

«امنیت اطلاعات» مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خراب‌کاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است.

در یک تعریف کلی و مرتبط با موضوع می‌توان گفت: «امنیت اطلاعات» به مجموعه‌ای از تدابیر، روش‌ها و ابزارهایی برای جلوگیری یا کاهش دسترسی و تغییرات غیرمجاز اشکال مختلف اطلاعات در نظام‌های نگهداری و تبادل سنتی و رایانه‌ای اطلاعات گفته می‌شود.

واژه‌های امنیت اطلاعات، امنیت رایانه‌ای و اطلاعات مطمئن، گاه به اشتباه به‌جای هم به‌کار برده می‌شود. اگرچه این‌ها موضوع‌های به‌هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یک‌پارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های

ظریفی بین آنها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله و موضوع‌هایی که تمرکز کرده‌اند بستگی دارد.

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است، بدون در نظر گرفتن شکل اطلاعات اعم از الکترونیکی، چاپ و یا اشکال دیگر (رشیدی،۱۳۹۱: ۱۴).

امنیت رایانه در حصول اطمینان از در دسترس بودن و عمل‌کرد صحیح سامانه رایانه‌ای تمرکز دارد، بدون نگرانی از اطلاعاتی که به‌وسیله این سامانه رایانه‌ای ذخیره یا پردازش می‌شود.

دولت‌ها، مراکز نظامی و امنیتی، شرکت‌ها، مؤسسه‌های مالی، بیمارستان‌ها و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصول‌ها، تحقیق‌ها، و وضعیت مالی گردآوری می‌کنند. بسیاری از این اطلاعات در حال حاضر روی رایانه‌های الکترونیکی جمع‌آوری، پردازش و ذخیره و در شبکه به رایانه‌های دیگر منتقل می‌شود. اگر اطلاعات محرمانه در مورد مشتریان یا امور مالی یا محصول جدید مؤسسه‌ای به‌دست رقیب بیفتد، این درز اطلاعات ممکن است به خسارت‌های مالی به کسب و کار، پی‌گرد قانونی یا حتی ورشکستگی منجر شود. حفاظت از اطلاعات محرمانه یک نیاز امنیتی، تجاری و در بسیاری از موارد نیز یک نیاز اخلاقی و قانونی است.

بحث امنیت اطلاعات در سال‌های اخیر به‌میزان قابل‌توجهی رشد و تکامل یافته است. راه‌های بسیاری برای ورود به این حوزه کاری به‌عنوان یک حرفه وجود دارد. موضوع‌های تخصصی گوناگونی در این حوزه وجود دارد که از جمله آن‌ها می‌توان به تامین امنیت شبکه(ها) و زیرساخت‌ها، تامین امنیت برنامه‌های کاربردی و پایگاه داده‌ها، آزمون امنیت، حسابرسی و بررسی سامانه‌های اطلاعاتی، برنامه‌ریزی تداوم تجارت و بررسی جرائم الکترونیکی و غیره اشاره کرد.

همان‌گونه که تعریف شد، امنیت اطلاعات یعنی حفظ محرمانگی، یک‌پارچه بودن و قابل دسترس بودن اطلاعات از افراد غیرمجاز.

محرمانگی: محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز.

یکپارچه بودن: یک‌پارچه بودن یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دست‌کاری غیرمجاز اطلاعات.

یک‌پارچگی وقتی نقض می‌شود که اطلاعات به‌صورت غیرمجاز تغییر داده می‌شود.

قابل دسترس بودن: اطلاعات باید زمانی که مورد نیاز افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سامانه‌های ذخیره و پردازش اطلاعات و شبکه‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد.

واپایش دسترسی به اطلاعات: برای حراست از اطلاعات، باید دسترسی به اطلاعات واپایش شود. افراد مجاز باید و افراد غیرمجاز نباید توانایی دسترسی داشته باشند.

کنترل دسترسی به اقدام‌هایی گفته می‌شود که منجربه حفاظت، مقابله، پیش‌گیری یا به حداقل رساندن خطرهای امنیتی است. این اقدام‌ها را می‌توان به سه دسته تقسیم کرد.

واپایش مدیریتی: واپایش مدیریتی (کنترل رویه‌ها) عبارتند از: سیاست‌ها، رویه‌ها، استانداردها و رهنمودهای مکتوب که به‌وسیله مراجع مسئول تأیید شده است.

قوانین و مقررات ایجاد شده از سوی نهادهای دولتی یک نوع از پایش مدیریتی محسوب می‌شوند (سادسکای،۱۳۸۳: ۱۷).

واپایش‌های مدیریتی پایه‌ای برای انتخاب و پیاده‌سازی پایش منطقی و فیزیکی است. کنترل‌های منطقی و فیزیکی ابزاری برای پیاده‌سازی و اعمال کنترل‌های مدیریتی هستند.

واپایش منطقی: پایش منطقی (کنترل فنی) استفاده از نرم‌افزار، سخت‌افزار و داده‌ها برای نظارت و کنترل دسترسی به اطلاعات و سامانه‌های رایانه‌ای. به‌عنوان مثال: گذرواژه، لیست‌های کنترل دسترسی و رمزنگاری داده‌ها نمونه‌هایی از کنترل منطقی هستند.

واپایش فیزیکی: برای حفاظت محیط ذخیره و بایگانی اطلاعات اعم از رایانه‌ای و غیررایانه‌ای، تجهیزات و نحوه دسترسی به آن‌ها است که جنبه فیزیکی دارند. به‌عنوان مثال: در، قفل، دوربین، موانع، نیروی‌های محافظ و غیره.

دسترسی به اطلاعات حفاظت‌شده باید به افراد، برنامه‌های رایانه‌ای، فرآیندها و سامانه‌هایی که مجاز به دسترسی به اطلاعات هستند محدود باشد. این مستلزم وجود سازوکارهایی برای کنترل دسترسی به اطلاعات حفاظت شده است. پیچیدگی سازوکارهای کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس‌تر و با ارزش‌تر نیاز به سازوکار کنترل دسترسی قوی‌تری دارند. اساس سازوکارهای کنترل دسترسی بر دو مقوله احراز هویت و تصدیق هویت است.

احراز هویت، تشخیص هویت کسی یا چیزی است. این هویت ممکن است ازسوی فرد ادعا شود یا ما خود تشخیص دهیم.

تصدیق هویت، عمل تأیید هویت است.

از سه نوع اطلاعات می‌توان برای احراز و تصدیق هویت فردی استفاده کرد:

۱. چیزهایی که افراد می‌دانند،[1]
۲. چیزهایی که افراد به‌همراه دارند،[2]
۳. چیزهایی که مربوط به خود کاربران است.[3]

نمونه‌هایی از چیزهایی که افراد می‌دانند شامل مواردی مانند رمز عبور می‌شود.

نمونه‌هایی از چیزهایی که افراد به‌همراه دارند شامل گواهی‌نامه رانندگی یا کارت‌های مغناطیسی می‌باشند.

1. Some things the user knows
2. Some things the user have
3. Some things the user are

کسی که فرد هست یا چیزهایی که مربوط به خود کاربران است[1] اشاره به فنون بیومتریک دارد. نمونه‌هایی از بیومتریک شامل اثرانگشت، اثر کف دست، صدا و اسکن شبکیه چشم و... هستند.

هر کدام از گزینه‌های بالا مزایا و معایبی دارند. کلمه‌های عبور ممکن است حدس زده شوند یا لو بروند اما به کاربر اجازه می‌دهد که قدرت خود را در اختیار شخص دلخواه دیگری قرار دهد. بسیاری از افراد به‌سادگی کلمات عبور را فراموش می‌کنند، به‌ویژه اگر به‌ندرت از آن‌ها استفاده کنند.

چیزهایی که کاربران در اختیار دارند می‌توانند گم یا دزدیده شوند، اما می‌توانند در صورت لزوم به شخص دیگری منتقل یا قرض داده شوند.

داده‌های نوع سوم تشخیص هویت، انعطاف ندارند، برای نمونه، نمی‌توان آن‌ها را از طریق تلفن به شخص یا جای دیگری منتقل کرد.

طراحان سامانه‌های امنیتی باید این سؤال را مطرح کنند که آیا کاربران باید توانایی انتقال اختیارشان را به دیگران داشته باشند یا خیر؟ پاسخ این سؤال در انتخاب نوع و روش شناسایی و تعیین هویت مؤثر است. به‌علاوه، روش‌های شناسایی می‌توانند به صورت ترکیبی نیز مورد استفاده قرار گیرند. برای مثال یک کارت و یک گذرواژه به‌همراه یکدیگر برای ورود به سامانه-های اطلاعاتی، حساب بانکی و... درخواست شود (دنینگ،۱۳۸۳: ۲۹).

موضوع اصلی این مقاله بررسی نوع سوم تشخیص و تأیید هویت یعنی تشخیص هویت افراد از طریق چیزهایی که مربوط به خود کاربران است و به اصطلاح به‌عنوان «داده‌های بیومتریکی[2]» شناخته می‌شوند.

1. Some things the user are
2. Biometric Data

بیومتریک: بیومتریک یا زیست‌سنجی به نوع خاصی از روش‌های امنیتی گفته می‌شود که در آن برای برقراری امنیت از خواص قابل اندازه‌گیری بدن انسان یا هر موجود زنده دیگر استفاده می‌شود. در این روش با استفاده از الگوریتم‌های ریاضی از اندام‌ها برداشت‌های ثابت و یکتایی می‌شود که می‌توان از آن به‌عنوان یک کلمه عبور یکسان و غیرقابل تقلید و گاه غیرقابل تغییر استفاده نمود.

واژه «بیومتریک» به طیف گسترده‌ای از فناوری‌هایی گفته می‌شود که هویت افراد را به کمک اندازه‌گیری و تحلیل ویژگی‌های انسانی شناسایی می‌کنند.

در یک تعریف عام‌تر، بیومتریک را علم و فناوری اندازه‌گیری و تحلیل آماری داده‌های بیولوژیکی معرفی کرده‌اند (Jain،85:1999) اما تعریف دقیق‌تر و فنی‌تر آنکه امروزه رایج شده به قرار زیر است:

هر خصوصیت فیزیولوژیکی یا ویژگی رفتاری منحصر به فرد و متمایز کننده، مقاوم و قابل سنجش که بتواند برای تعیین یا تأیید خودکار هویت افراد به‌کار رود، بیومتریک نام دارد (هاتف،۲۵:۱۳۸۶).

سامانه‌های بیومتریک داده‌هایی از کاربر را ذخیره و هر بار که لازم شد برای تعیین هویت و تصدیق اصالت فرد این داده‌ها را مقایسه می‌کنند.

سامانه‌های بیومتریک: سامانه بیومتریک به‌طور اساسی یک سامانه تشخیص الگو است که با به‌دست آوردن داده‌های بیومتریک از یک فرد عمل می‌کند. این سامانه یک مجموعه ویژگی از داده‌های به‌دست آمده را استخراج کرده و با الگوهای پایگاه داده خود مقایسه می‌کند (جلالی و رجبی نسب، ۵۶:۱۳۸۷). از هر ویژگی با شرایط زیر به‌عنوان مشخصه بیومتریک استفاده می‌شود:

۱. **جهانی بودن**[1]: هر فرد باید این ویژگی را داشته باشد.

۲. **تمایز**[1]: هر دو فرد باید برحسب این ویژگی، متفاوت باشد.

1. Universality

۳. **دوام**[2]: این ویژگی باید در یک دوره زمانی برای یک فرد ثابت باشد.

۴. **قابلیت جمع‌آوری**[3]: این ویژگی را بتوان به‌صورت کمّی اندازه‌گیری کرد.

۵. **قابلیت پذیرش**[4]: به مفهوم مقبولیت آن در جوامع گوناگون است (Jain،1999:38).

آزمایش زیست‌سنجی: آزمایش زیست‌سنجی در سامانه بیومتریک شامل سه گام است:

الف- ثبت مشخصات: کاربران با سنجش‌های اولیه در سامانه ثبت‌نام می‌شوند. این عمل در چند مرحله برای ثبت اطلاعات دقیق انجام می‌گیرد.

ب- مقایسه: گام بعدی مقایسه نمونه با الگوی مرجع است. در این مرحله تعیین سطح مناسب خطای مجاز[5] به‌ویژه برای سنجش رفتاری از اهمیت ویژه‌ای برخوردار است.

پ- به‌روز رسانی: تمامی سامانه‌های بیومتریک به‌خصوص آن‌هایی که از ویژگی‌های رفتاری کاربر استفاده می‌کنند، باید متناسب با قابلیت به‌روز رسانی الگوی مرجع طراحی شده باشند.

انواع فنون و روش‌های بیومتریک

فنون بیومتریک به دو دسته تقسیم می‌شود:

الف- فنون رفتاری[6]: مانند امضانگاری، الگوی تایپ، صدا، دست خط و ... .

ب- فنون فیزیولوژیکی[7]: مانند اثرانگشت، اسکن دست یا هندسه دست، اسکن عنبیه، اسکن شبکیه، اسکن صورت یا هندسه صورت و ... .

الف- فنون رفتاری: فنون رفتاری، الگوهای رفتاری مشخص یک فرد را تشخیص و شناسائی می‌کند. در این روش، طرز انجام کاری به‌وسیله کاربر سنجیده می‌شود. در زیر به چند نمونه از آن اشاره می‌کنیم:

1. Distinctiveness
2. Permanence
3. Collectability
4. Acceptability
5. Tolerance
6. Behavioral
7. Physiometric

۱- نحـوه تایـپ کـردن[1]: روشـی کـه یـک نفـر بـا صـفحه کلیـد تایـپ مـی‌کنـد، یکـی از بیومتریک‌هـای رفتـاری اسـت. تایپیسـت‌هـای مـاهر بـه‌طـور تقریبـی خیلـی زود از الگوهـای تایپ کردن شـان تشـخیص داده مـی‌شـوند. در ایـن روش، زمـان پـائین نگـه‌داشـتن کلیـدها، سـرعتِ زدن کلیـدها، میـزان خطـا در زدن کلیـدها و غیـره از عوامـل مهـم اسـت. پیـاده‌سـازی‌هـای فعلـی بـه دلیـل مشـکلات یکسـان نبـودن صـفحه کلیـدها و تـأخیر نرم‌افزارها در جواب‌دهی، به سامانه آزمایشگاه محدود شده‌اند.

هزینه پائین و عملیات شفاف، این روش را به یک روش بسیار جذاب و ساده برای کاربردهایی همانند محافظت از سامانه‌های خبره تبدیل کرده است.

۲- تشخیص صدا[2]: در این سامانه، صدای کاربران، نوع و ضرب‌آهنگ آن سنجیده و رتبه‌بندی می‌شود. سپس این عدد با اعداد مشابه پیشین مقایسه می‌گردد. از جمله موارد استفاده آن اعطای اجازه ورود به مکان‌های محافظت شده است. این سامانه بیشتر برای تأیید هویت از راه دور به‌وسیله تشخیص صدا در ارتباط‌های تلفنی مورد استفاده قرار می‌گیرد.

با وجود افزایش کیفیت این سامانه، دقت آن هنوز به اندازه سامانه‌های دیگر بیومتریک نیست زیرا تشخیص صدای فرد ممکن است مورد تأثیر شرایط فیزیکی وی (خستگی، سرماخوردگی، خواب‌آلودگی و غیره) تغییر کند.

به‌علاوه، ابزار مورد استفاده مانند نوع تلفن نیز می‌تواند روی فرایند تشخیص صدا اثر بگذارد. از این‌رو، از این سامانه اغلب همراه با سایر روش‌های بیومتریک استفاده می‌شود.

۳- شناسایی از طریق دست‌خط: در نگاه نخست، استفاده از دست‌خط برای شناسایی افراد ایده چندان مناسبی به نظر نمی‌رسد چرا که بسیاری از انسان‌ها می‌توانند دست‌خط دیگر افراد را در مدت کوتاهی و با چندبار تمرین به‌خوبی تقلید کنند. ممکن است کپی از امضای یک نفر

1. Scan key-Stroke
2. Scan-Voice

یا جعل دست‌خط او آسان و امکان‌پذیر به‌نظر برسد اما این سامانه هوشمند فقط به‌شکل نهایی امضا یا کلمه توجه نمی‌کند بلکه آن‌را تحلیل می‌کند. میزان فشار قلم روی کاغذ و سرعت و آهنگ نوشتن و ترتیب شکل دادن به حروف را بررسی و حتی عادت‌های نوشتاری را ثبت می‌کند. به‌عنوان مثال نقطه یا علامتی که اغلب بعد از نوشتن کلمه یا متنی گذاشته می‌شود برخلاف شکل‌های ساده حروف که به‌آسانی جعل می‌شوند، تقلید این خصایص فردی از آنچه که به‌نظر می‌آید بسیار مشکل‌تر است، حتی اگر شخصی از امضای خاصی کپی داشته باشد و عین آن‌را روی صفحه رسم کند، به احتمال بسیار زیاد، سامانه امضا را نخواهد پذیرفت.

ب- فنون فیزیولوژیکی: در این حالت، یک خصوصیت فیزیکی مانند اثرانگشت یا الگوی عنبیه مورد سنجش قرار می‌گیرد. در زیر به چند نمونه از آن‌ها اشاره می‌کنیم:

۱- اثرانگشت[1]: این روش از قدیمی‌ترین روش‌های آزمایش تشخیص هویت است، هرچند در گذشته‌های دور تنها در زمینه جرم‌شناسی از آن استفاده می‌شد. سامانه‌های بیومتریک می‌توانند جزئیاتی از اثرانگشت مانند تقاطع‌ها، کناره‌ها و برجستگی‌ها را ذخیره و سپس آن‌ها را با نمونه‌های موجود در مرجع مقایسه کنند.

برای استفاده از اثرانگشت از پویشگر[2] مخصوصی استفاده می‌شود. این اسکنرها انواع متفاوتی دارند. بعد از اینکه انگشت روی صفحه اسکنر قرار گرفت، بسته به نرم‌افزار استفاده شده، اثر انگشت پویش شده و نقاط کلیدی آن تعیین شده و با الگوی اولیه تطبیق داده می‌شود. با توجه به اینکه زمان مقایسه بعد از مدتی که حجم مقایسه‌ها زیاد شد، بالا می‌رود و برای کمتر کردن این زمان، ابتدا نقاطی را به‌عنوان نقاط کلیدی برای دسته‌بندی پویش‌های موجود استفاده و در زمان انطباق از همین کلیدها استفاده کرده و زمان مقایسه پایین آورده می‌شود.

1. Scan- Finger
2. Scaner

هرچند که تحلیل اثرانگشت بعضی از افراد مانند کارگرانی که کارهای سخت با دست‌های خود انجام می‌دهند یا افرادی که به انواع مواد مخدر اعتیاد دارند، مشکل است ولی در کل در بسیاری از موارد از اثرانگشت استفاده‌های موفقی صورت می‌پذیرد.

امروزه این پویشگرها نه‌تنها در اداره‌های پلیس بلکه روی صفحه کلیدها و حتی موش‌واره رایانه‌ها وجود دارند و از آن‌ها در موارد مختلفی استفاده می‌شود، به‌عنوان مثال می‌توان با استفاده از امکانات نرم‌افزاری، رایانه را قفل کنیم و در صورتی سامانه رایانه قفل را باز کند که اثرانگشت شما را روی صفحه پویشگر خود پویش کند.

این امکان وجود دارد که از پویش اثرانگشت به‌جای تایپ گذرواژه در باز کردن رایانامه[1]های الکترونیکی‌مان استفاده کنیم یا در تجارت الکترونیک یا تغییر موجودی در بانک‌های برخط[2] از آن استفاده ببریم.

از پویش اثرانگشت برای گرفتن اجازه ورود به مکان‌های امنیتی یا دسترسی به اطلاعات طبقه‌بندی شده استفاده می‌شود. کاربران می‌توانند با داشتن یک پویش اثر انگشت، ورود به رایانه شخصی خود و دسترسی به داده‌های آن را محدود کنند.

پرداخت پول با اثرانگشت جدیدترین روشی است که به‌تدریج جای چک، کارت اعتباری و ابزارهای الکترونیکی را خواهد گرفت.

اثرانگشت از برآمدگی‌ها و فرورفتگی‌ای تشکیل شده است که بسته به وضعیت قرار گرفتن آن‌ها ویژگی‌های مختلفی به‌وجود می‌آید. تا کنون هجده ویژگی برای اثرانگشت شناخته شده است که دو ویژگی مهم آن، انتهای برآمدگی و دوشاخه شدن برآمدگی است که در اصطلاح به آن‌ها مینوتیا می‌گویند.

1. Email
2. Online

ساختار توپولوژیکی مینوتـای یـک اثرانگشـت منحصـربه‌فـرد بـوده و بـا گذشـت زمـان تغییـر نمی‌کند. در نتیجه مـی‌تـوان تشـخیص اثرانگشـت را بـر مبنـای تطبیـق سـاختار توپولـوژیکی مینوتیـا اسـتوار کـرد. در یـک تصـویر انگشـت بـا کیفیـت بـه‌طـور نسـبی خـوب در حـدود هفتاد تـا هشـتاد مینوتیـا وجـود دارد کـه البتـه ایـن تعـداد در تصـویرهای جزئـی بـه حـدود بیست تا سـی ویژگـی کـاهش مـی‌یابـد، امـا بـاز هـم بـا ایـن تعـداد مـی‌تـوان عمـل تطبیـق اثرانگشـــت را انجـــام داد (اشـــراقی، ۳۶:۱۳۹۰). بیشـــتر ســـامانه‌هـــای تشـــخیص اثرانگشـــت، ساختاری بـر مبنـای مینوتیـا دارنـد. در ایـن سـامانه‌هـا سـه مرحلـه اساسـی بـرای تشـخیص وجود دارد که عبارتند از:

۱. پیش‌پردازش
۲. استخراج مینوتیا
۳. تطبیق مینوتیا

مرحله اول برای افزایش کیفیت تصویر انجام می‌گیرد، مرحله دوم برای استخراج ویژگی‌های تصویر و مرحله آخر برای مقایسه مورد استفاده قرار می‌گیرد.

۲- پویش چشم

۱. پویش چشم به دو صورت است:
۲. پویش عنبیه[1]
۳. پویش شبکیه[2]

پویش عنبیه: در عنبیه‌نگاری از الگوی پیچیده و منحصر به‌فرد عنبیه که حتی در چشمان راست و چپ یک انسان هم متفاوت هستند، تصویربرداری می‌شود. ادعا می‌شود خطای تشخیص این

1. Iris-Scan
2. Retina- Scan

سامانه‌ها در حد یک در چند ده میلیون است. کپی‌برداری مصنوعی از عنبیه به‌علت ویژگی‌ها و تعداد خصوصیات قابل سنجش آن به‌طور تقریبی غیرممکن است (26:2004,Bowyer).

پویش نمودن عنبیه به‌وسیله دوربین‌های مادون قرمز یا دوربین‌های تصویربرداری صورت می‌گیرد.

پویش‌گرهای عنبیه رگه‌های موجود در عنبیه چشم را می‌سنجند که برای این‌کار بایستی کاربر از فاصله سی سانتیمتری یا بیشتر برای چند ثانیه به دوربین نگاه کند. در ضمن عینک و لنزهای تماسی کاربران با سامانه سنجش و شناسائی عنبیه تطابق دارد و مشکلی در این زمینه به وجود نمی‌آورد.

برخی از مزایای عنبیه برای شناسایی افراد:

- قابل‌رویت از خارج است.
- منحصر به‌فرد بودن به دلیل پیچیدگی ترکیبی.
- در طول دوران زندگی پایدار می‌باشند.
- دارای ساختار شکل گرفته قبل از تولد(ماه هفتم از دوران بارداری).
- برخی از معایب عنبیه برای شناسایی افراد:
- کوچک بودن هدف (یک سانتیمتر) برای دست‌یابی از فاصله‌ای حدود یک متر.
- متحرک بودن هدف.
- قرار گرفتن عنبیه در پشت سطحی منعکس کننده، مرطوب و منحنی.

تأثیر مژه‌ها، عدسی‌ها و انعکاس‌های روی آن.

۱. نبود وضوح تصویر به دلیل فروافتادگی پلک‌ها.
۲. تغییر شکل غیرارتجاعی به دلیل تغییر اندازه مردمک.

پویش شبکیه: شبکیه افراد مختلف دارای طرح و الگویی یکتا از رگ‌های خونی است و می‌توان از الگوی رگ‌های خونی که در شبکیه وجود دارند برای تشخیص افراد استفاده کرد.

در پویش شبکیه با استفاده از دوربین مخصوص، الگوی رگ‌های خونی اسکن می‌شود. برای این‌کار از لیزر مادون‌قرمز کم‌قدرت استفاده می‌شود.

هر شبکیه هم مانند عنبیه دارای الگوی منحصر به‌فردی است که در سامانه‌های شبکیه‌نگاری به‌وسیله یک پرتو نوری پویش می‌شود. از این سامانه‌ها در کاربردهای بسیار امنیتی و حساس استفاده می‌شود.

کالبدشکافی و یکتایی شبکیه: شبکیه از بافت‌های گیرنده‌ای است که از لایه‌های مختلفی تشکیل شده است. همچنین شبکیه از میلیون‌ها گیرنده نوری تشکیل شده که عملکرد آنها عبارت است از جمع‌آوری اشعه‌های نوری است که به آن فرستاده می‌شود و تبدیل این نورها به پالس‌های الکتریکی است که با عبور از عصب نوری به مغز رسیده و در آنجا این پالس‌های الکتریکی به تصویر تبدیل می‌شود.

به‌علت اینکه شبکیه در مکانی درون چشم قرار گرفته است و در مقابل محیط خارج از چشم نیست به عنوان یک روش تشخیص هویت پایدار قلمداد می‌شود.

فن‌آوری دستگاه‌های پویش‌گر: دستگاه‌های اسکن شبکیه از سه بخش عمده تشکیل شده‌اند:

۱) قسمت تصویربرداری و پردازش موج

این بخش شامل دوربینی برای تصویربرداری و سپس تبدیل تصویر پویش شده از شبکیه به شکل دیجیتال است.

۲) قسمت تطبیق دهنده

این بخش شامل یک سامانه رایانه‌ای اعتبارسنجی و تشخیص هویت استفاده کننده است.

۳) قسمت نمایش دهنده

در این بخش ویژگی‌های یکتای شبکیه به‌صورت یک قالب نمایش و ذخیره می‌شود مزیت روش شبکیه در این است که شاخص‌های ژنتیکی تعیین کننده الگوی شبکیه نیستند. این موضوع باعث می‌شوند که شبکیه دارای ویژگی‌های منحصر به‌فرد قوی باشد. از شبکیه تا چهارصد نقطه منحصر به‌فرد می‌توان اطلاعات استخراج کرد که نسبت به اسکن اثر انگشت که سی تا چهل نقطه است بسیار روش دقیق‌تری است.

منابع خطاها در پویش شبکیه

۱. همکاری نکردن و هرگونه حرکت از سمت استفاده کننده در مرحله اخذ تصویر می‌تواند باعث خطا شود.
۲. رعایت نکردن فاصله مشخص شده به‌وسیله دستگاه.
۳. لنز کثیف دستگاه اسکن شبکیه.
۴. تداخل نوری به‌وسیله محیط خارجی.
۵. ابعاد مردمک استفاده کننده.
۶. روشنایی زیاد محیط باعث کاهش نوری می‌شود که از طریق مردمک به شبکیه و بالعکس منتقل می‌شود. این امر باعث نپذیرفتن به‌وسیله دستگاه می‌شود.

۳- هندسه دست[1]: برخی از سامانه‌های بیومتریک نیز مبتنی‌بر پویش دست هستند. این پویش می‌تواند خطوط کف دست، عروق‌خونی پشت دست یا هندسه دست را شامل گردد. در مورد اخیر از تصاویر بعدی دست و اندازه‌گیری پهنا، عرض و طول انگشتان و بند انگشتان استفاده می‌شود به این ترتیب که کاربر دست خود را در فضای مشخص شده قرار می‌دهد و دوربین از بالا و کنار با تهیه تصاویر لازم اطلاعات خواسته شده را دریافت می‌کند. برخلاف تصور اولیه، این سامانه از ساختار یافته‌ترین فن‌آوری‌های روز به‌شمار می‌رود و از صحت عملکرد بالایی برخوردار است.

1. Hand-Scan

شکل کف دست بعد از مدتی با گذشت سال و با بالا رفتن سن تغییر می‌کند و نیز جراحت‌ها نیز باعث عوض شدن شکل کف دست می‌شود بنابراین در استفاده از این روش باید اسکن به‌دست آمده درمواقع لزوم و نیز بعد از یک دوره زمانی به‌روز شود و پویش جدیدی برای شناسایی افراد ایجاد شود. استفاده از این روش در مواردی مفید است که به طور مستمر مورد استفاده قرار گیرد و افراد مورد شناسایی با این روش در دسترس باشند. این روش به‌علت اینکه سطح بزرگی را مورد مقایسه قرار می‌دهند دارای ضریب اطمینان بالایی هستند.

۴- چهره‌نگاری[1]: کوشش‌های بشر برای تعبیه ابزار مکانیکی قابل‌اطمینان برای شناسایی ویژگی‌های رفتاری و فیزیولوژیکی اشخاص، تاریخچه‌ای بس طولانی و رنگین دارد. به‌طور مثال در دوران ویکتوریا با الهام از پیدایش جرم‌شناسی که برای شناسایی زندانیان و تبه‌کاران وجود داشت، سرفرانسیس گالتون فهرست‌های مختلفی از ویژگی‌های برجسته صورت تهیه کرده بود. همچنین وی تعدادی انتخاب کنندگان خودکار مکانیکی برای اندازه‌گیری ویژگی‌های صورت تهیه کرده و یک آزمایشگاه اندازه‌گیری ویژگی‌های بدن انسان در کنزینگتون جنوبی تاسیس نموده بود تا براساس سامانه پزشک فرانسوی به‌نام آلفونس برتیلون هر یک از مجرمان را در یکی از ۸۱ طبقه‌ای که او ایجاد کرده بود قرار دهد. از دیگر مشخص کنندگان ویژگی‌های فیزیولوژیکی و رفتاری که در طول تاریخ به‌کار گرفته شده‌اند می‌توان ابعاد جمجمه، طول انگشت، اندازه‌گیری ویژگی‌های مختلف هندسی صورت و غیره را نام برد.

در روش چهره‌نگاری از ویژگی‌های متمایز و منحصر به‌فرد چهره استفاده می‌شود. بنای کار این روش بر دو نوع تصویربرداری ویدیویی و حرارتی است که روش اول از رواج بیشتری برخوردار است و طرز به‌کارگیری آن نیز نسبت به روش دوم آسان‌تر است.

اساس کار این روش مبتنی‌بر محل نقاط کلیدی صورت از قبیل چشم‌ها، دهان و سوراخ‌های بینی است. در روش دوم، براساس گرمای نقاط مختلف صورت کاربر، اطلاعات آنها در سامانه

1. Facial-Scan

نگه‌داری شده، سپس با اطلاعات موجود در بانک اطلاعات مقایسه می‌گردد تا درستی آن مشخص شود. این روش به‌علت استفاده از سخت‌افزار و نرم‌افزارهای گران قیمت، هزینه زیادی دارد ولی قابلیت اعتماد بالایی دارد. در این روش نیز مانند روش اسکن کف دست نیاز به‌هنگام شدن اطلاعات وجود دارد (فولادوند،۱۳۸۹: ۴۱).

روش‌های استخراج ویژگی‌ها از چهره

در سال‌های اخیر روش‌های مختلفی برای استخراج ویژگی‌های مهم و موثر برای شناسایی چهره مورد بررسی قرار گرفته است، این روش‌ها به سه دسته کلی تقسیم‌بندی می‌شوند: (Bowyer،2004:51).

الف- ویژگی‌های ظاهری: ویژگی‌های ظاهری شامل مختصات اجزای چهره، مانند چشم‌ها، بینی، بافت‌ها و نواحی مختلف چهره است که همان ویژگی‌های ظاهری چهره هستند. در استخراج این ویژگی‌ها از تصویر، محدودیت‌های فراوانی وجود دارد.

ب- ویژگی‌های جبری: هر تصویر می‌تواند به‌صورت یک ماتریس تلقی شده و سپس عملیات جبری و تبدیل ریاضی مختلف روی آن اعمال گردد. ویژگی‌های جبری، حاصل این فرایند بوده و اغلب نشانگر خواص ذاتی یک تصویر است. از عملیات مهم روی ماتریس تصویر، تحلیل مؤلفه‌های اساسی است. این تبدیل یکی از روش‌های مهم برای استخراج ویژگی‌های جبری از تصویر چهره است که بر مبنای بردارهای ویژه ماتریس کواریانس بنا نهاده شده است. بردارهای ویژه ماتریس، بیان کننده توزیع جبری ماتریس و ثابت‌های هندسی بوده و می‌تواند برای استخراج ویژگی از تصویر به‌کار برده شود (Bowyer،2004:31).

از دیگر روش‌های جبری، روش تجزیه مقادیر منفرد است. می‌توان نشان داد که تجزیه مقادیر منفرد ماتریس یکی از روش‌های مؤثر برای استخراج ویژگی از ماتریس تصویر است. تجزیه مقادیر منفرد در فشرده‌سازی و پردازش موج نیز مورد استفاده قرار می‌گیرد.

ج- ویژگی‌های آماری نقاط تصویر: با توجه به دو بعدی بودن تصاویر و در نظر گرفتن نقاط تصویر به‌صورت داده‌های آماری، می‌توان از مشخصات آماری نقاط، برای توصیف تصویر استفاده کرد. در این روش اغلب از ویژگی‌هایی استفاده می‌شود که دارای توانائی کافی برای توصیف تصویر بوده و ضمن غنای اطلاعاتی، از پایداری خوبی نیز برخوردار باشد. یکی از روش‌های آماری مهم استفاده از روش خود بستگی موضعی با درجه بالا است.

بیومتریک‌های دیگر: عوامل دیگری هم‌اکنون مورد استفاده قرار گرفته‌اند که درحال‌حاضر، به علل مختلف وسعت کاربرد آنها محدودتر است و از جمله می‌توان به بیومتریک‌های زیر اشاره کرد:

نحوه راه رفتن، بوی بدن، دی.ان.ای[1]، چهره‌نگاری سه‌بعدی، چهره‌نگاری حرارتی، شکل گوش، عروق لاله گوش، دست‌خط، اندازه‌گیری‌های جمجمه، بافت پوست و بازتابش نور از آن، نحوه گرفتن اشیاء با دست و ... .

نحوه عملکرد سامانه‌های بیومتریک

۱. یک کاربر با ارایه داده‌های بیومتریک مورد نیاز، در سامانه ثبت‌نام می‌کند.
۲. الگوهای بیومتریک پردازش شده حاصل از داده‌ها، در سامانه ذخیره می‌شود.
۳. به‌منظور تأیید یا تعیین هویت، مشخصه بیومتریک افراد دوباره دریافت می‌شود.
۴. الگوهای تأیید هویت با یک یا چند الگوی ثبت شده در سامانه مقایسه می‌شود.
۵. نتایج مقایسه با سطح آستانه اطمینان سامانه مقایسه می‌شود.
۶. نتیجه نهایی اعلام می‌شود.

کاربردهای عمومی سامانه‌های بیومتریک: در یک تقسیم‌بندی عمومی بیومتریک سه نوع امنیت را به ارمغان می‌آورد:

۱. امنیت فیزیکی (امنیت دسترسی به هر فضای فیزیکی ممکن).

1. D.N.A

۲. امنیت فضای سایبر (امنیت دسترسی منطقی به شبکه رایانه‌ای یک سازمان).

۳. امنیت تعاملات (امنیت انجام هرگونه تراکنش مالی و اعتباری).

با توجه به سه حوزه امنیتی اشاره شده در بالا به تعدادی از کاربردهای سامانه‌های بیومتریک در این حوزه‌ها اشاره می‌شود:

شناسایی مجرمان

انگشت‌نگاری جز متداول‌ترین فن‌آوری‌های بیومتریک مورد استفاده در این حوزه است. مراجع قضایی به‌طور تقریبی در تمام جهان اثرانگشت را به‌عنوان یک مدرک مستند در مباحث جرم‌شناسی به رسمیت می‌شناسند. به‌عنوان مثال بانک داده‌های یک‌پارچه سازمان جاسوسی آمریکا[1] است، هم‌اکنون دارای میلیون‌ها ثبت ده انگشتی است که روزانه هزاران جست‌وجو برای شناسایی مجرمان، در آن انجام می‌شود. این بانک داده با دیگر بانک‌های اطلاعاتی موجود در سامانه‌های نظارتی و پیگردی آمریکا در ارتباط است. همچنین هم‌اکنون اطلاعات این بانک با اطلاعات بانک اطلاعات بیومتریک اسکاتلندیارد انگلستان هم به اشتراک گذاشته شده تا امکان استفاده همزمان از اطلاعات این منابع میسر شود.

تجارت الکترونیک، تلفنی، خودپردازها، پایانه‌های فروش

تراکنش‌های مالی و اعتباری، تأیید هویت مشتریان و دسترسی به حساب‌ها یا صندوق امانات و... از جمله مهم‌ترین کاربردهای بیومتریک در حوزه تجارت الکترونیک به‌شمار می‌رود که تاکنون مجموعه متنوعی از بیومتریک‌های مختلف برای این منظور استفاده شده است. بخشی از این کاربردها ممکن است حفاظت‌های داخلی یا زیرساختی از قبیل کنترل دسترسی به اماکن امنیتی یا شبکه‌های رایانه‌ای برای جابه‌جایی سرمایه‌های الکترونیکی باشد. کاربرد گسترده‌تر شاید حفاظت از اسرار و هویت افراد باشد. به‌ویژه نخستین کاربردی که به ذهن خطور می‌کند، حفاظت خودپردازها،

1. IAFIS

کـارت‌هـای اعتبـاری و چـک‌هـا، بـا شناسـه‌هـای بیـومتریکی اسـت. امـروزه کـارت‌هـای خودپرداز با رمزهای عبور حفاظـت مـی‌شـوند کـه چـالش‌هـای امنیتـی و کـاربری فراوانـی را درپـی داشـته اسـت. در ایـن شـرایط فـن‌آوری بیومتریـک رفتـه رفتـه جـایگزین رمزهـای عبور می‌گردد.

در کشور ژاپن رگ‌نگاری کف دست، در کانادا عنبیه‌نگاری، در ایالات متحده آمریکا و کشورهای اروپائی انگشت‌نگاری و چهره‌نگاری پرکاربردترین بیومتریک‌ها در حوزه بانک‌داری الکترونیک[1] محسوب می‌شود.

دسترسی به رایانه‌های شخصی و شبکه

انگشت‌نگاری پرکاربردترین بیومتریک در این حوزه است. در سال‌های اخیر مایکروسافت سامانه عامل خود را مجهز به رابط برنامه کاربردی بیومتریک کرده است.

دسترسی فیزیکی

نسل جدید سامانه‌های ساعت‌زنی و کنترل حضور و غیاب از جمله ابزارها و تجهیزاتی است که به فن‌آوری بیومتریک مجهز شده است. انگشت‌نگاری، دست‌نگاری و چهره‌نگاری از جمله پرکاربردترین بیومتریک‌ها در این بخش هستند.

شناسایی شهروندان: طیف وسیعی از بیومتریک‌ها با فن‌آوری‌های گوناگون و با اهداف مختلف در شناسائی شهروندان مورد استفاده قرار می‌گیرند که انگشت‌نگاری در صدر آن‌ها قرار دارد.

نظارت: با توجه به ماهیت کاربری نامحسوس چهره‌نگاری، این فن‌آوری کارکرد فوق‌العاده‌ای در نظارت محسوس و نامحسوس دارد. بسیاری از خیابان‌های ناامن شهر لندن هم‌اکنون به دوربین‌های مدار بسته‌ای مجهز شده است که امکان تشخیص هویت افراد سابقه‌دار یا تحت پیگرد به‌وسیله آنها به‌راحتی ممکن شده است.

- کمک به ایجاد سامانه بانک اطلاعاتی[1] امن.

1. E-Banking

- جلوگیری از دسترسی افراد فاقد صلاحیت به منابع اطلاعاتی حیاتی، حساس و مهم کشور.
- کمک به برقراری ارتباط امن برای تبادل اطلاعات.
- تأیید هویت بازماندگان، مجروحان، متوفیان، گم‌شدگان و آمارگیری سریع و دقیق در زمان بحران و غیربحران.

دلایل به‌کارگیری فن‌آوری بیومتریک در آینده: پیاده‌سازی بیومتریک با درخواست الزام‌آور و بین‌المللی دولتی در حوزه کاربردی کارمندان، شهروندان و اتباع خارجی.

- آسانی و تسریع خدمات در حوزه‌های مختلف زندگی مانند استفاده در گذرنامه‌ها، کارت‌های شناسایی و....
- افزایش کاربرد کارت‌های شناسایی چند منظوره، به‌خصوص کارت‌های مغناطیسی و هوشمند.
- علاقمندی‌های دولتی و تجاری به محصول‌های پیشرفته‌ای که موجب شناسایی هویت سارقان را فراهم کند.
- احساس نیاز به این‌گونه سامانه‌ها به‌وسیله اقشار مختلف جامعه به دلایل مختلفی مانند ایجاد امنیت بیشتر حریم‌ها، جایگزین شدن سامانه‌های قدیمی برای ایجاد دقت بالاتر و توانایی پردازش حجم اطلاعات بیشتر.
- تقاضا برای محصول‌های مدیریت تشخیصِ هویت متمرکز(بانک‌های اطلاعاتی یک-پارچه).
- افزایش کاربرد وسایل کنترل از راه دور و بی‌سیم برای دسترسی به شبکه‌های نفوذپذیر یا منابع برخط.

1. Information Center

مزایای فناوری‌های بیومتریک: فن‌آوری‌های بیومتریک بسته به نوع کاربردشان در امور امنیتی و کنترلی نسبت به فن‌آوری‌های اسلاف خویش(پین‌کدها، کارت‌های شناسایی، علامت‌های ویژه و ...) مزیت‌های فراوانی دارند که بخشی از مهم‌ترین آن‌ها عبارتند از:

۱.غیرقابل سرقت.

۲.غیرقابل فراموشی.

۳.غیرقابل حدس زدن.

۴.بی‌نیازی به نگهداری ویژه.

۵.راحتی و سرعت استفاده.

۶.کاهش زیان‌های ناشی از تقلب، سرقت و...

۷.امکان تعیین هویت اصلی و واقعی افراد و شناسایی مظنونین.

۸.کاهش هزینه‌های امنیتی در خصوص به‌کارگیری نیروی انسانی ورزیده.

۹.امکان جست‌وجوی سریع در بانک‌های اطلاعاتی و لیست‌های سیاه (تحت پیگرد) (مهرابیان،۱۳۸۵: ۷۹)

نتیجه‌گیری

طراحی و پیاده‌سازی یک محیط ایمن برای ذخیره، گردش و تبادل اطلاعات یکی از چالش‌های اساسی در عصر حاضر محسوب می‌گردد و این مهم در پدافند غیرعامل به‌عنوان یک اصل، در سیاست‌گذاری‌های این حوزه مورد تأکید قرار گرفته است. این اقدام موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، آسانی مدیریت بحران و درنهایت موجب ارتقای پایداری ملی در مقابل اقدام‌های فیزیکی، تهدیدهای امنیتی و حمله‌های سایبری عناصر دشمن برای دسترسی به اطلاعات طبقه‌بندی شده می‌گردد.

امروزه تنوع تهدیدها، ضرورت به‌کارگیری وسایل قابل اطمینان، سریع و غیرتهاجمی برای تشخیص هوشمند هویت اشخاص برای تعیین و تأیید دسترسی به اسنادومدارک، حضور

کارکنان مجاز و جلوگیری از حضور افراد غیرمجاز در اماکن حساس را ملزم کرده است. بدیهی است سازمان‌های مختلف که به‌طور طبیعی مسؤول تامین امنیت اطلاعات خود می‌باشند نیازمند به استفاده از فن‌آوری‌ها و وسایل با مشخصات ذکر شده هستند.

در سازمان‌های اطلاعاتی، دفاعی و امنیتی هم که دارائی‌های ارزشمندی به‌نام اطلاعات را نگهداری می‌نمایند یا دارای اماکن و تأسیسات حیاتی و حساس متنوعی می‌باشند، ضرورت به‌کارگیری ابزارها و روش‌های قابل اطمینان، سریع و غیرتهاجمی برای مدیریت امن اطلاعات و کنترل دسترسی‌ها بیش از سایر سازمان‌ها ضرورت پیدا کرده است.

با عنایت به توضیحات ارائه شده در این مقاله، روش‌های فیزیولوژیکی و رفتاری فن‌آوری بیومتریک با برخورداری از محاسن و قابلیت‌های منحصر به‌فرد خود، در صورت به‌کارگیری قانونمند و استفاده صحیح و دقیق می‌تواند به‌عنوان یکی از ابزارهای قابل اتکا در حوزه ارتقای امنیت اطلاعات مورد بهره‌برداری قرار گیرد.

نگرش کاربردی به پیاده‌سازی اصول پدافند غیرعامل و توجه به نیازمندی‌های ارائه شده زیر، به‌کارگیری فن‌آوری بیومتریک هم‌راستا با «ارتقای امنیت اطلاعات» ارزیابی می‌شود:

۱) تأکید مقام معظم رهبری به مقوله مهم امنیت و ترسیم آن به‌عنوان پیش‌نیاز اساسی هرگونه پیشرفت علمی، اقتصادی، اجتماعی، فرهنگی و سیاسی کشور.

۲) پیش‌بینی مجامع معتبر علمی جهان همچون دانشگاه ام.آی.تی در ذکر فن‌آوری بیومتریک به‌عنوان یکی از ده فن‌آوری جدید تغییر دهنده چهره دنیا در آینده.

۳) روند رو به رشد کاربرد فن‌آوری بیومتریک در زمینه تأمین امنیت و کنترل دسترسی فیزیکی و منطقی به منابع مالی، اطلاعاتی، شبکه رایانه‌های مراکز حساس و همچنین صدور مدارک شناسایی قابل اطمینان.

۴) استفاده الزامی از این فن‌آوری در آینده‌ی بسیار نزدیک برای تعاملات بین‌المللی با سایر کشورهای جهان.

۵) لزوم پرهیز یا امکان برون‌سپاری امر مشاوره، تهیه، پیاده‌سازی و کاربست فن‌آوری بیومتریک به مؤسسه‌ها و شرکت‌های بیگانه به‌ویژه برای پروژه‌های ملی و دفاعی کشور.

۶) احتمال بروز تهدیدها امنیتی غافل‌گیر کننده به دلیل تسلط آمریکا و رژیم اشغال‌گر قدس بر این فن‌آوری برای پیش‌رو بودن آن‌ها در طراحی و تولید سامانه‌های بیومتریک و تدوین استانداردهای آن.

۷) محدودیت‌های پیش‌رو به‌ویژه تحریم‌های موجود در زمینه فروش برخی محصول‌های پیشرفته فن‌آوری بیومتریک به ایران، به دلیل ماهیت حساس امنیتی و دفاعی این کاربردها.

۸) وجود توان و قابلیت‌های علمی، پژوهشی و سخت‌افزاری بالقوه قابل‌اعتنای داخلی برای مشاوره، تولید، خرید و کاربست فن‌آوری بیومتریک و امکان بهره‌گیری از آن در صورت شناسایی و سرمایه‌گذاری متناسب برای پرورش و رشد گروه‌های متخصص.

۹) پرهیز از فرصت‌سوزی و تکرار تجربه ابتلا به مشکلات ناشی از تأخیر در بهره‌گیری از فرصت‌های پیشرفت(برنامه‌ریزی و کسب آمادگی لازم در مواجهه با فن‌آوری‌های نو).

۱۰) فقدان اجماع و اراده علمی و یک‌پارچه برای بومی‌سازی، به‌کارگیری و توسعه این فن‌آوری و به عبارتی اختلال و سردرگمی فراروی استفاده از این فن‌آوری.

منابع

۱.اشراقی،حمیدرضا .(۱۳۹۰). ***تامین فیزیکی***؛ چاپ اول، تهران، مرکز آموزشی و پژوهشی شهید صیاد شیرازی.

۲.جلالی، علی اکبر- رجبی‌نسب، مزدک .(۱۳۸۷). ***بیومتریک ابزار امنیت شهروند هزاره سوم***.

۳.جلالی‌فراهانی، غلامرضا .(۱۳۸۸). ***مبانی نظری پدافند غیرعامل با رویکرد تهدیدات جدید***، پژوهشکده مستقل پدافند غیر عامل دانشگاه جامع امام حسین (ع).

۴.دنینگ، داروتی الیزابت رابلینگ .(۱۳۸۳). ***جنگ اطلاعات و امنیت***، چاپ اول، تهران، پردازش هوشمند علائم.

۵.رشیدی، محمدرضا .(۱۳۹۱). ***امنیت گوگل***، تهران، انتشارات گویا آی تی.

۶.سادسکای جورج و دیگران .(۱۳۸۳). ***راهنمای امنیت فناوری اطلاعات***، ترجمه مهدی میردامادی،زهرا شجاعی و محمدجواد صمدی، انتشارات دبیرخانهٔ شورای عالی اطلاع‌رسانی.

۷.عابدی، محمدحسین .(۱۳۸۸). ***مدیریت حفاظت و امنیت اطلاعات***، انتشارات انستیتو ایز ایران، چاپ اول.

۸.فولادوند، زهره .(۱۳۸۹). ***تکنولوژی بیومتریک در امنیت اطلاعات***، پروژه سمینار دانشجوئی.

۹.مهرابیان، هاتف .(۱۳۸۵). تشخیص هویت بر مبنای تحلیل تصاویرعنبیه چشم، ***پایان‌نامه کارشناسی مهندسی برق***.

۱۰.نوروزی، محمدتقی .(۱۳۸۵). ***فرهنگ دفاعی-امنیتی***، تهران، نشر سنا.

۱۱.هاتف، مهدی، مقاله بیومتریک .(۱۳۸۶). ***دوماهنامه توسعه انسانی پلیس***، سال چهارم، شماره۱۲، مرداد و شهریور.

*12. A. Jain, **'Personal identification in a networked society'**, 1999.*

*13.K.W. Bowyer , **'Face Recognition and the Security versus Privacy**.*