وزارة التعليم العالي والبحث العلمي

جامعة الفرات الاوسط

المعهد التقني /السماوة

قسم تكنولوجيا المعلومات والاتصالات

مدرس المادة :م.م بيداء هادي محمد سعودي

https://au.edu.sy/images/courses/dentistry/1-1/129_computer-in-dentistry.pdf

المحاضرة الثالثة

أمنية الحاسبات والبيانات

COMPUTER & DATA SECURITY

أركان امن المعلومات :

١ -السريةCONFIDENTIALITY

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات ألاشخاص غير مصرح لهم بالاطلاع عليها أو الكشف عنها. على سبيل المثال، بطاقة الائتمان والمعاملات التجارية على شبكة الانترنت يتطلب رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر النجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الارسال، وذلك بالحد من الاماكن ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصاالت المطبوعة)، وذلك بتقييد الوصول إلى الاماكن التي يتم تخزين الرقم والبيانات بها. اماإذا كان الطرف غير المصرح به قد حصل على رقم البطاقة بأي شكل من الاشكال ،وبذلك فقد تم انتهاك مبدأ السرية في حفظ وتخزين البيانات.

خرق السرية يتخذ أشكالا عديدة. تجسس شخص ما على شاشة الكمبيوتر لسرقة كلمات سر الدخول ،أو رؤية بيانات سرية لديك بدون علم منك يمكن أن يكون خرقا للسرية. إذا الكمبيوتر المحمول يحتوي على معلومات حساسة عن موظفي الشركة هو سرق أو بيع، يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر الهاتف هو انتهاك لمبدأ السرية إذا كان الطالب غير مخول أن يحصل على المعلومات.

السرية أمر ضروري)لكنها غير كافية(للحفاظ على الخصوصية من الناس الذين يخترقون الأنظمة لسرقة المعلومات الشخصية في لنظام التعليق.

٢ ــالتكاملية وسلامة المحتوى INTEGRITY:

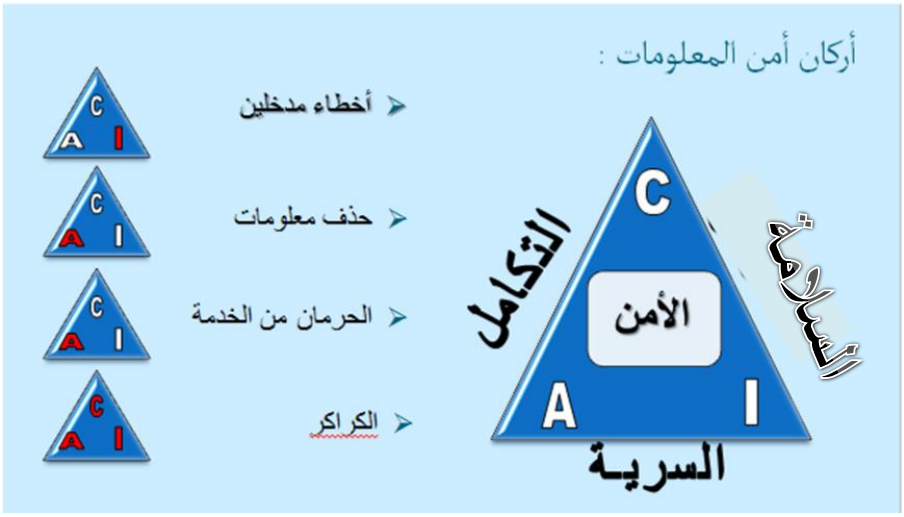
في مجال أمن المعلومات، السالمة تعني الحفاظ على البيانات من التغيير والتعديل من الأشخاص الغير مخول لهم بذلك. عندما يقوم شخص بقصد أو بغير قصد انتهاك سالمة أو الإضرار أو حذف ملفات البيانات الهامة وهو غير مخول بذلك فهذه انتهاك لسالمة البيانات، وعندما يصيب فيروس كمبيوتر ويقوم بتعديل بيانات أو اتلافها فهذا انتهاك سالمة بيانات، وعندما يكون الموظف قادرا على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم غير مصرح له بتخريب موقع على شبكة الإنترنت، وهلم جرا.

٣- توفر قاعدة البياناتAVAILABILITY :

يهدف أي نظام للمعلومات لخدمة غرضه، يجب أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات، والضوابط الأمنية المستخدمة لحمايته، وقنوات الاتصال المستخدمة للوصول إلى ذلك يجب أن يعمل بشكل صحيح. توافر نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات، ومنع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، اونظام الترقيات والتحديث. ضمان توافر ينطوي أيضا على منع الحرمان من الخدمة الهجمات.

وهكذا فإن الحفاظ على سرية المعلومات وسلامتها أمر مهم ولا ريب، لكن هذه المعلومات تصبح غير ذات قيمة إذا كان من يحق له الاطلاع عليها لا يمكنه الوصول إليها أو أن الوصول إليها يحتاج وقتاً طويلا. لذا فإن المتخصصون يرون أن لأمن المعلومات خصائص ثلاثة على درجة واحدة من الاهمية، وهذه المكونات هي:

١



جرائم المعلوماتية:

هي تعبير شامل يشير إلى جريمة تتعلق باستعمال إحدى وسائل تقنية المعلومات لغرض خداع الاخرين وتضليلهم، أو من أجل تحقيق هدف معين لجهة معينة.

تكبد جرائم المعلوماتية الحكومات والمنشآت خسائر تقدر بمليارات الدولارات سنوياً.

تصنيف جرائم المعلوماتية

١-جرائم هدفها نشر المعلومات:

مثل الحصول على أرقام البطاقات الائتمانية، والحسابات المصرفية ومعلومات استخباراتية.

٢- جرائم هدفها نشر معلومات غير صحيحة:

مثل نشر المعتقدات والأفكار الخاطئة .

٣- استخدام تقنية المعلومات كوسيلة لاداء الجريمة:

مثل تزوير بطاقات الائتمان والتحويل بين الحسابات المصرفية.

٤-جرائم لها عالقة بانتشار تقنية المعلومات:

مثل قرصنة البرامج الاصلية والتي تكون أسعارها ٥٠٠٠$ لتباع بأقل من ١٠$

المخترقون:

إن معظم الدخلاء هم هواة حواسيب وخبراء حواسيب حيث الوصول غير المخول بالنسبة لهم نوع من لعبة عقلية لا تقاوم.

المخترقون نوع hackers :

هم هواة حواسيب يتمتعون بالمغامرة بأنظمة الحاسوب (وبأنفسهم) إلى أبعد الحدود. إنهم يجرون التجارب بالبرامج لمحاولة لاستكشاف الإمكانيات غير المشار إليها في دليل البرمجيات. يعدل المخترق الأنظمة للحصول على أعظم أداء ممكن. وأحياناً يحاولون تتبع الضعف والثغرات في أمن النظام. عندما يحاول hackers الوصول غير المخول فإنهم نادراً ما يخربون البيانات أو يسرقون البيانات الموجودة.

١- يحاول فقط أن يتعرف على كيفية عمل النظام والبرامج لكي يساعد في تطويرها وتحسينها.

٢- لديه القدرة الكاملة على اختراق أنظمة التشغيل عبر الأنترنت.

٣- يقوم الهاكر بحل المشاكل و بناء الاشياء، و يؤمن بالعمل التطوعي.

٤- الهاكر دائما عمله بناء ومفيد و ينفع الاخرين.

المخترقون نوع Crackers :

هم مخترقون من نفس النوع السابق أصبحوا مهووسين بكسب الدخول إلى أنظمة الحواسيب ذات المستوى العالي من الأمان. وهم أيضاً عامةً ال يقصدون تخريب أو سرقة البيانات ولكن تكرار وتعقيد هجماتهم يمكن أن يتسببوا في إزعاج كبير لمدراء النظام.

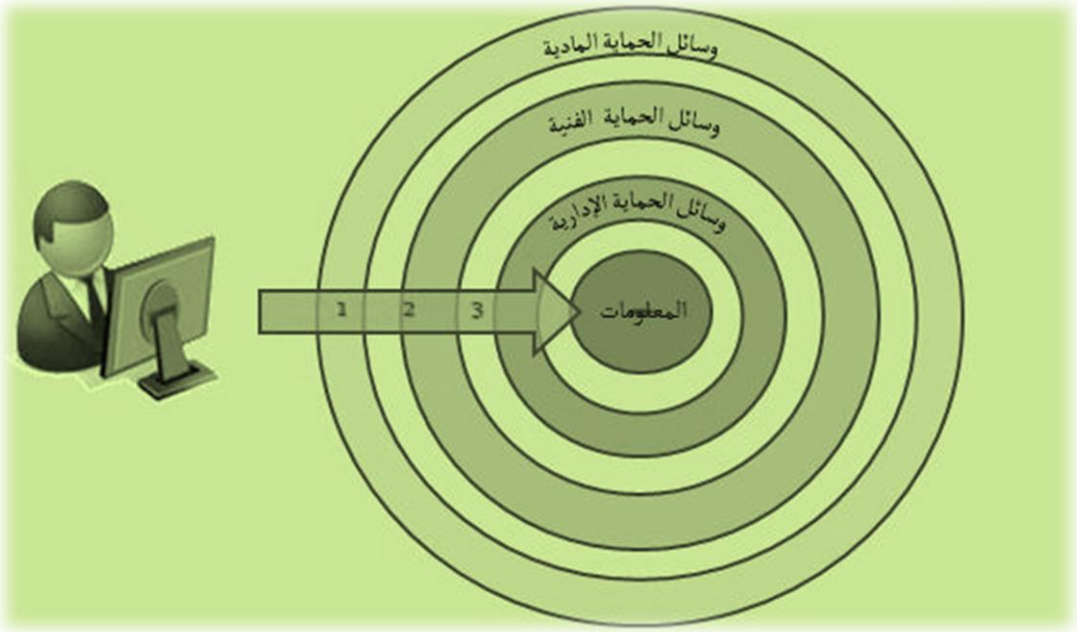
١- يمتلك القدرة على اختراق أنظمة التشغيل والبرامج الغير مجانية والتلاعب في برمجتها وإعطاؤها رقم خاص لكي تعمل.

٢- ويقوم بكسر الأنظمة الأمنية لاهداف تخريبية، فقد يكون هدفه سرقة معلوماتك أو في أسوأ الاحيان القضاء على النظام المعلوماتي الكتروني، بشكل كلي.

٣- كثير منهم يقوم بسرقة البرامج و توزيعها مجانا لهدف، فمنهم من يضع ملف الباتش بين ملفات هذا البرنامج.

٤- الكراكر دائما عمله تخريبي ولا ينفع سوى نفسه أو من يدفع له.

وسائل الحماية:



أ- وسائل الحماية المادية:

وهي الأجزاء المحسوسة من وسائل الحماية.

من أمثلتها:

١- (الكاميرات) الفيديو أو الفوتوغرافية
٢- أجهزة الإنذار .
٣- الجدران والأسوار والمفاتيح.
٤- بطاقات دخول الموظفين.
٥- أجهزة اكتشاف الأصوات والحركة.

ب- وسائل الحماية الفنية:

وهي تقنيات تحديد وإثبات هوية المستخدم وصلاحياته ومسئولياته.
من أمثلتها:
١- كلمة المرور.٢-القياس الحيوي.٣-التشفير.٤-الجدران النارية.٥-البرامج المضادة للفيروسات.٦-التوقيع الإلكتروني.

ج- وسائل الحماية الإدارية:

وهي إعداد وصياغة سياسات أمن المعلومات وتتضمن:

- **تشريعات داخل المنشأة لتنظيم أمن المعلومات وتحديد المسؤوليات والأدوار.**
- **تحدد ما هو مسموح به وما هو غير مسموح به للتعامل مع المعلومات ومع نظم المعلومات.**

من أمثلتها:

١-اتفاقية صلاحيات المستخدم وقبول استخدام النظام.

٢- الخصوصية.

٣- كلمات المرور.

٤- البريد الإلكتروني.

بعض الأمثلة لوسائل تحقيق أمن المعلومات:

١ـ كلمة المرور

أو كلمة السر هي تشكيلة من الحروف الأبجدية والأرقام والرموز الأخرى تمكن من يعرفها من الوصول أو استعمال مورد أو خدمة محمية .ومن الضروري عدم إفشاء كلمة السر لتفادي وقوعها بين أيدي آخرين فتفتح لهم الباب إلى ما لم يكن بوسعهم الوصول إليه بدونها. تقنيا، تعتبر كلمة السر من وسائل الحماية الضعيفة مقارنة مع وسائل أخرى.

لاختيار كلمة المرور:

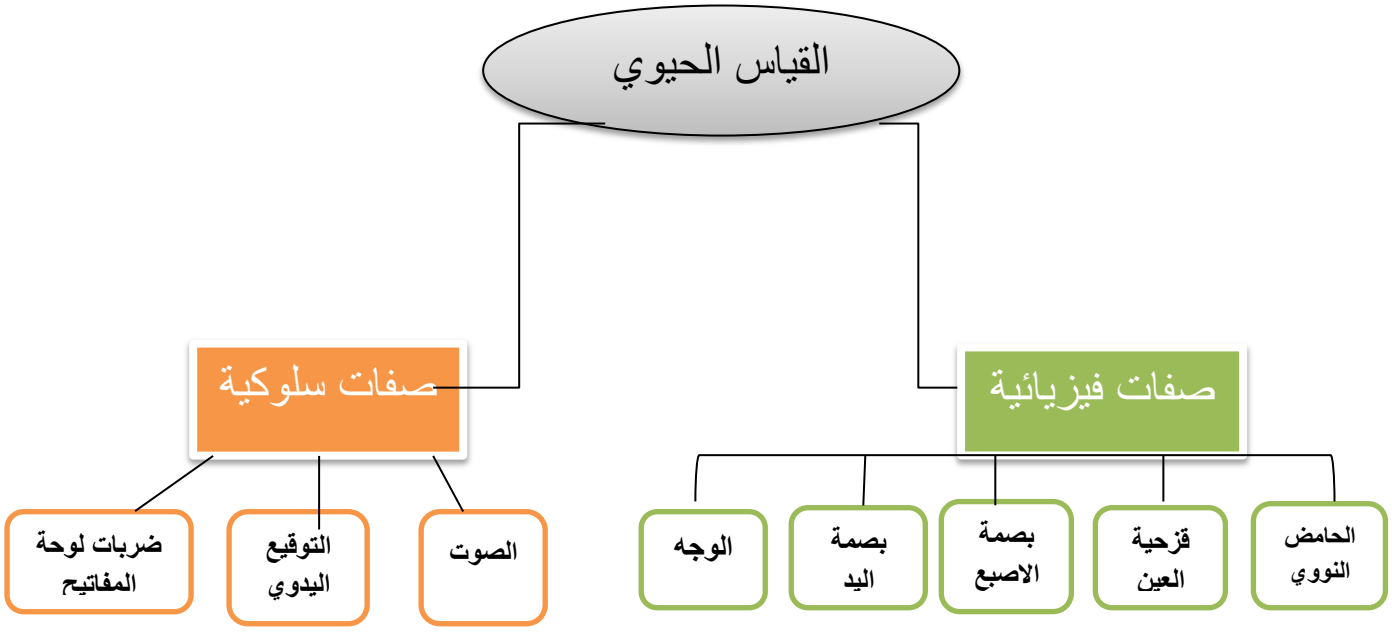
١ـ يفضل أن تحتوي على أحرف وأرقام.
٢ـ يفضل أن لا تقل عن ٨ خانات.
٢ـ يفضل أن ال تكون مشهور ومتداولة.
٣ـ يمكن استخدام معادلة بسيطة لإنشاء كلمة المرور

٢ ـ القياس الحيوي :Biometrics

Biometricsهي كلمة إغريقية مكونة من جزئيين "BIO" ومعناها الحياة و "METRICS" ومعناها قياس. والتعريف الدقيق للقياس الحيوي : هو العلم الذي يستخدم التحليل الإحصائي لصفات الإنسان الحيوية وذلك للتأكد من هويتهم الشخصية باستخدام صفاتهم الفريدة.

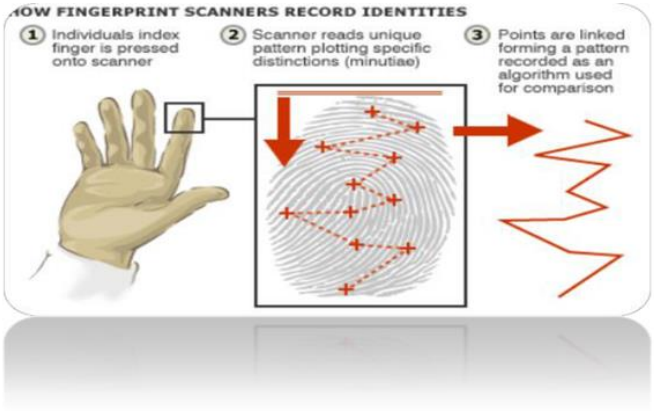
انواع القياس الحيوي

١ـ الصفات الفيزيائية: وهي الصفات التي تتعلق بجزء من جسم الإنسان.
٢ـ الصفات السلوكية: وهي الصفات التي تتعلق بسلوك الإنسان.



بصمة الإصبع :Fingerprint Scanning

أكثر الأنظمة شيوعا في الاستخدام وخاصة بين المستخدمين لاجهزة تقنية المعلومات .بصمة الاصبع تمسح ضوئيًا باستخدام قارئات خاصة، ومن الامثلة على هذه القارئات :أجهزة تربط بالكمبيوتر ، أو تأتي مدمجة مع الفأرة.



بصمة اليد :Hand Geometry

يستخدم هذا النظام منذ سنوات عديدة وبشكل خاص في أنظمة متابعة الحضور والانصراف وتسجيل الوقت .يعطي هذا النظام توازنًا جيدًا بين ألاداء والدقة وسهولة الاستخدام .ومن

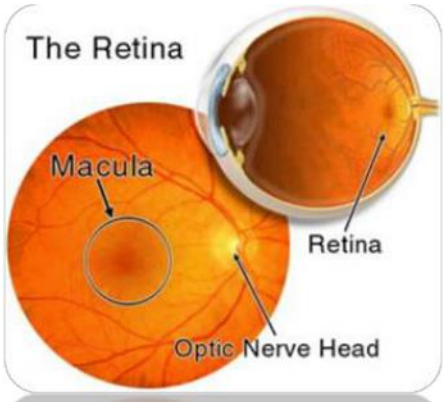
السهولة دمجه في أنظمة أخرى . توضع اليد على الجهاز الماسح في المكان المخصص لها، ويقوم النظام بفحص تسعين صفة من بينها شكل اليد ثلاثي الابعاد 3D، طول وعرض الأصابع، وكذلك شكل مفاصل الأصابع.

قزحية العين :Iris Scanning

يعتمد النظام المستخدم لقزحية العين على ثباتها حيث أنها الجزء الذي لا يتغير من الجسد .ولها ميزة أيضًا أنها مرئية عن بعد، ليست كصفة الشبكية .أيضًا قزحية العين اليسرى تختلف عن العين اليمنى لنفس الشخص.، ولا يحتاج المستخدم أن يقرب هذه العدسات من عينه، وهي بالتالي تعطي دقة عالية مع سهولة الاستخدام.

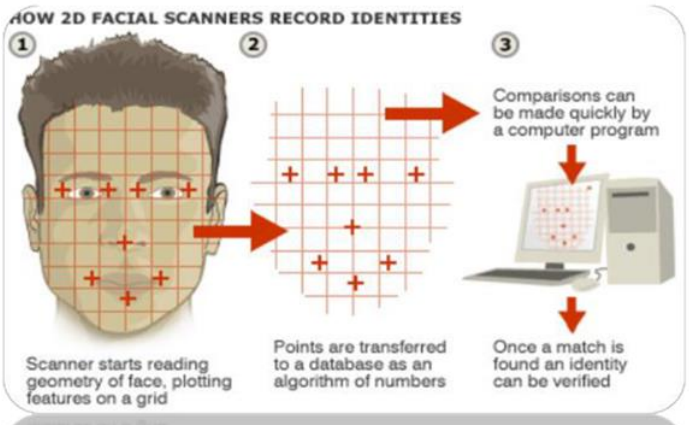
شبكية العين :Retina Scanning

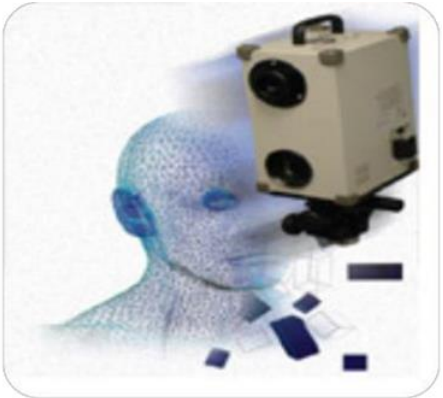
هذه الطريقة تستخدم مصدر ضوء منخفض لعمل مسح للشعيرات الدموية خلف العين. عيب هذه الطريقة أن المستخدم يجب أن ينظر ويركز على الماسحة وهذا يسبب للمستخدم عدم الرغبة للتعامل مع النظام.



الوجه :Facial Scanning

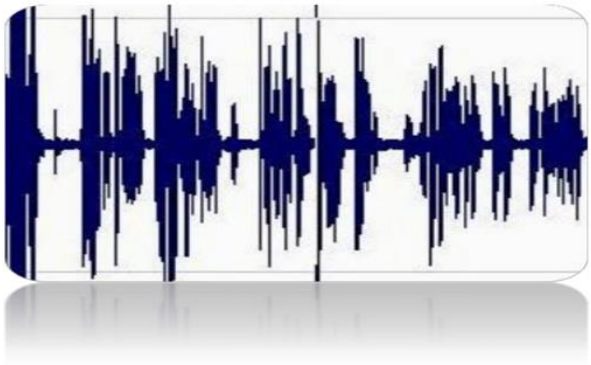
هذا النظام يعتمد على أخذ صورة كاملة للوجه من آلة تصوير، وقيام النظام بمقارنتها مع ما خزن فيه مسبقًا .مازالت هذه التقنية في أوج التطوير، وما هو موجود حالياً من الأنظمة المعتمدة على صورة الوجه لاتعطي دقة عالية





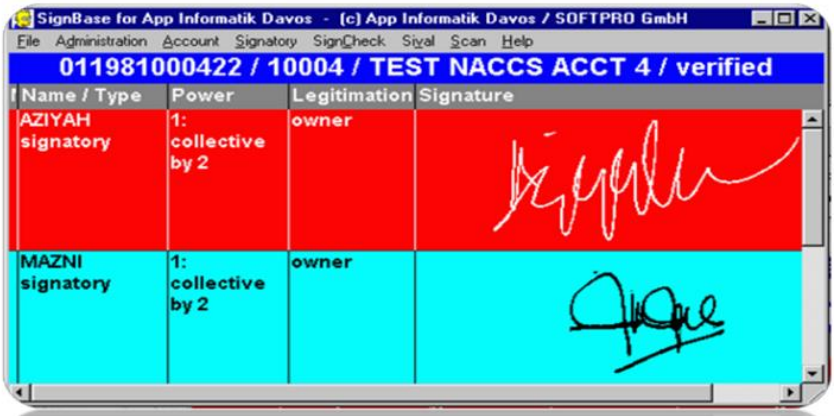
الصوت :Voice Verification

في هذه الايام، برامج تدقيق الصوت تعد من الاضافات الشائعة لاجهزة الكمبيوترات الخاصة لدى معظم الشركات والبنوك .لكن أنظمة القياس الحيوي ألمعتمدة على الصوت، فإنها تحلل ترددات الصوت بشكل اكثر دقة لكي تعطي نتائج صحيحة يعتمد عليها ولذلك يجب أن تكون بيئة هذا النظام هادئة، حيث أن أي ضجة تؤثر على النتيجة و أجهزة هذا النظام قد تكون مستقلة بحد ذاتها أو مدمجة مع أنظمة الهاتف التي قد تساعد في مجالات عديدة منها الانظمة المصرفية



التوقيع اليدوي :Signature Verification

هذا النظام يعتمد على الطريقة التقليدية لتوقيع الشخص، ولكنها تتم من خلال توقيع الشخص على شاشة حساسة للمس باستخدام قلم ضوئي. ويتم من خلالها تحويل توقيعه إلى شكل رقمي ومن ثم مقارنته مع ما خزن مسبقًا في النظام.



لحمض النووي :DNA Scanning

هذا النظام يعتمد على الشريط الوراثي للشخص .DNA وهو نظام معقد جدًا ويستحيل تغييره بين الأشخاص، وهذا النظام مكلف جدًا لذلك قليلً ما يستخدم.

ضربات لوحة المفاتيح :keystroke Dynamics

هذا النظام يقوم تسجيل ضربات الشخص على لوحة المفاتيح .ومن خلال هذه العملية يقوم بمراقبة الوقت بين ضرب مفتاح والانتقال الأصابع لضرب مفتاح آخر .وكذلك يراقب الوقت الذي يأخذه المستخدم وهو ضاغط على المفتاح .وحيث أنه يجب على المستخدم أن يتذكر أسم المستخدم والرقم السري.

مميزات القياس الحيوي :

يوفر لنا القياس الحيوي عدد من المزايا منها:

١- الأمن والخصوصية:

يمنع الأشخاص الآخرين من الدخول الغير مصرح على البيانات الشخصية.
إيقاف سرقة الهوية مثل استخدام البطاقات الائتمانية أو الشيكات المسروقة.

٢- البديل لحمل الوثائق الثبوتية مثل:

بطاقة الهوية الوطنية ، رخصة القيادة ، بطاقة الائتمان.

٣- البديل لحفظ وتذكر الأرقام السرية.

٤- البديل لحمل المفاتيح للدخول إلى:

السيارات، المنازل ، المكاتب

٥- تأمين سرية العمليات المالية مثل:

-مكائن الصراف الآلي ATM ، التجارة الإلكترونية.