Análisis de Sistemas de Identificación Personal para su uso en Sistemas Automatizados de Kioscos Electrónicos

Carlos Alfonso Trejo Villanueva[1], Ávila Camacho Francisco Jacob[2] y Adolfo Ramírez Meléndez[3]

Resumen

La identificación personalizada de cada individuo ha sido un tema de gran importancia para la gestión social y los sistemas particulares. Los sistemas automatizados necesitan un elemento de identificación para que los usuarios hagan un uso elocuente del mismo, por lo que el presente trabajo realiza un análisis sobre las características de las tres principales tendencias de identificación personal para su uso en sistemas automatizados de kioscos electrónicos, en los que se describen sus propiedades, costos, elementos de seguridad y finalmente se propone una recomendación de implementación basado en el equilibrio de estos parámetros y las características de cada sistema a desarrollar.

Acerca de los autores...

[1] Alumno de la Maestría en Ingeniería en Sistemas Computacionales, Tecnológico de Estudios Superiores de Ecatepec.

[2 y 3]Docente de la División de Sistemas Computacionales, Tecnológico de Estudios Superiores de Ecatepec.

[1]foligator@hotmail.com
[2]jacob@avilacamacho.com

Tecnológico de Estudios Superiores de Ecatepec

Palabras Clave: Sistemas de información, Sistemas de identificación, Biometría, Tendencias tecnológicas, Sistemas RFID

Introducción

Desde hace más de 100 años, ha sido una necesidad la identificación de los individuos que componen un grupo de la sociedad o inclusive dentro de la humanidad misma. Poder registrar asistencia por nuestra credencial, identificar los productos a través de lectores de códigos de barras, ingresar a sistemas de transporte público con tarjetas, abrir accesos con la huella digital, desbloquear los teléfonos con la imagen de nuestro rostro, comienzan a ser sistemas tan comunes en la actualidad que perdemos casi la perspectiva de los avances tecnológicos que están implícitos en ellas así como del abaratamiento de dicha tecnología que la ha puesto al alcance de la mayoría de nosotros.

La pregunta ahora es: ¿Hacia dónde van las tecnologías de identificación personal en la actualidad?, considerando que la tendencia actual de la información y los sistemas que la manejan tienen a globalizarse y a tener un dominio más público, pretendiendo también que dicha información pueda ser utilizada en el dominio de la nube y el IoT, principalmente.

Principios y fundamentos de la identificación personal

La identificación personal es un tópico que surge mucho tiempo atrás. Entre 1870 y 1900, se realizarón muchos trabajos referentes a dicho tema; trabajos como el de William James Herchel en 1877 quién fue el primer personaje en reconocer la individualidad de la huella dactilar postulando que estas son perennes tomando sus propias impresiones durante un periodo de 28 años, o la investigación realizada por Alphonse Bertillon en 1893, médico francés que creo un novedoso sistema denominado antropometría, el cual consistía en la identificación de delincuentes por medio de sus características físicas (longitud de miembros, diámetro del cráneo, distancia de separación de globos oculares, etc.), han permitido crear sistemas de identificación basados en dichos principios.

Un Sistema de Identificación Personal, permite verificar la identidad de las personas durante eventos sensibles, a través de diferentes medios y técnicas, las cuales permiten ofrecer la seguridad y fiabilidad de reconocimiento único de cada individuo registrado en él.

Las tecnologías actualmente utilizadas en la identificación personal se han diversificado permitiendo que los aspectos y procesos de reconocimiento se basen principalmente en rasgos biométricos o en dispositivos personales únicos que permiten asegurar el correcto funcionamiento en el objetivo de la caracterización de los usuarios del sistema y su correcta validación.

Preparación de la contribución

La identificación personal debe tener una serie de elementos que puedan ser caracterizados o parametrizados de forma tal que permitan su almacenamiento, recuperación y comparación rápida, integra y confiable para ser considerado un sistema viable.

Los sistemas automatizados por su parte, han crecido y se han convertido en sistemas comunes y cotidianos con los que se han familiarizado usuarios en su

vida cotidiana. Encontrar máquinas para pagar boletos de estacionamiento, sistemas de prepago para servicios de transporte público, cajeros electrónicos automatizados, expendedoras de productos, etc., es una realidad con la que convivimos cada día; ahora el elegir un sistema de identificación personal para los usuarios de estos sistemas es un tópico de suma importancia.

Las tecnologías que son utilizadas en la actualidad son diversas, pero podemos concentrarlas en:

Sistemas de identificación por credenciales de usuario (login y password)

Sistemas de identificación por pruebas de comportamiento e historial (validaciones vía correo electrónico y SMS o sistemas Captcha)

Sistemas de identificación a través de bandas magnéticas y microcircuitos.

Sistemas de identificación por chips de radiofrecuencia (RFID y NFC).

Sistemas de identificación por rasgos biométricos (dactilar, retina, rostro, palma).

Cada uno de estos sistemas tiene un fundamento de funcionamiento basado en un elemento de identificación único que puede ser clasificado, categorizado y diferenciado de manera precisa para poder ser utilizado para un fin específico dentro de la estructura del sistema de identificación y validación.

Cabe recalcar que la elección del sistema de reconocimiento personal varía en función y uso dependiendo de las características tecnológicas, la infraestructura del sistema computacional y del sistema de comunicación principalmente de las necesidades de seguridad por las que fue diseñado y destinado en su uso.

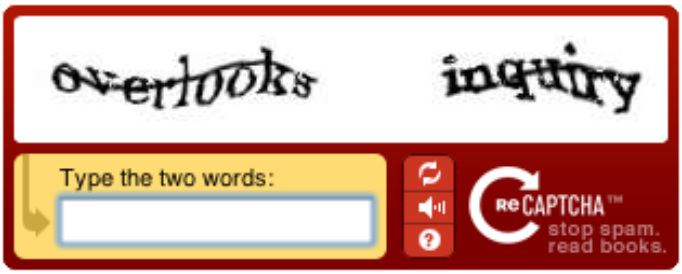

Figura 1

Imagen del Sistema Captcha - Completely Automated Public Turing test to tell Computers and Humans Apart (University, 2010).

Sistemas de identificación basados en la entrega de credenciales y comportamiento

Este tipo de sistemas se basa en la identificación de individuos a través de credenciales de acceso a los sitios de información. En la generación de credenciales se ha seguido la tendencia por hacerlas más complejas y personales; contraseñas utilizadas en el pasado como "1234" o las fechas de nacimiento de los usuarios fueron catalogadas como las perores en su uso; los prestadores de servicios de acceso y grandes empresas de tecnologías de la información como Google, Microsoft y Apple, proponen e inclusive controlan

la generación de contraseñas efectivas y seguras que traten de evitar en la medida de lo posible la irrupción abrupta de los accesos personales de los usuarios, por lo que se dan recomendaciones básicas para la generación de contraseñas como:

Tratar de utilizar un mínimo de caracteres.
Utilizar combinación de mayúsculas y minúsculas.
Agregar caracteres numéricos.
Utilizar en medida de lo posible uno o más caracteres especiales.
Asociar las contraseñas con elementos de recuperación como preguntas secretas o frases para recordar
No utilizar la misma contraseña en todos los sitios o accesos del usuario.

Estas recomendaciones no siempre son suficientes, pero se estima que mejoran el rendimiento, administración y seguridad de los sistemas de información de forma considerable.

Otro elemento que ha sido adicionado a la validación por credenciales es la identificación de patrones de comportamiento o identificación por sistemas alternos. Entre estos procesos podemos identificar la validación de nuevos accesos a través de la confirmación de identificación por correos electrónicos, por mensajes de texto SMS, o el acceso mismo a través de credenciales de otros sistemas (como Facebook o Gmail de Google); inclusive, cotidianamente podemos percatarnos de este tipo de reconocimiento cuando nos llegan múltiples avisos de sesiones abiertas en plataformas operativas nuevas, avisos de operaciones realizadas en portales bancarios, del intento de accesos a sistemas de usuario, a los cambios en la configuraciones de los perfiles personales y de seguridad entre otros, con los que se pretende establecer un patrón de comportamiento del usuario y reconocer las operaciones poco frecuentes y que ponen en riesgo la integridad de su información o su identificación.

Figura 2

Esquema de descripción de debilidad de contraseñas en el sitio Hotmail (Acunetix, 2015).

Sistemas de identificación basados claves asignadas por tarjetas y por dispositivos identificadores

La identificación de individuos a través de dispositivos de identificación personales portables, como por ejemplo tarjetas con bandas magnéticas, tarjetas con chips de identificación por contacto o tarjetas de identificación por radiofrecuencia RFID y NFC, así como tokens y stickers con circuitos impresos.

Este tipo de sistemas pretende asignar un identificador único portable para los usuarios de un sistema contemplando la pertinencia de cada clave asignada y evitando la duplicidad. Los sistemas de banda magnética y chip de identificación han sido utilizados por instituciones que requieren mucha seguridad como los sistemas bancarios, y sistemas de identificación por tarjetas inalámbricas son utilizados en la actualidad en los sistemas de transporte público así también como en instituciones particulares y de acceso a edificaciones de servicios públicos.

Los sistemas de identificación por chips de identificación mediante RFID y NFC comienzan a ser una tendencia y popularizarse por su eficiencia, durabilidad, confiabilidad y bajo costo. Este tipo de sistemas tiene una durabilidad reconocida consecuencia de la falta de friccion o contacto físico entre tags y lectores, además de la eficiencia en la comunicación de datos resultado de las velocidades de transferencia entre los dispositivos de comunicación.

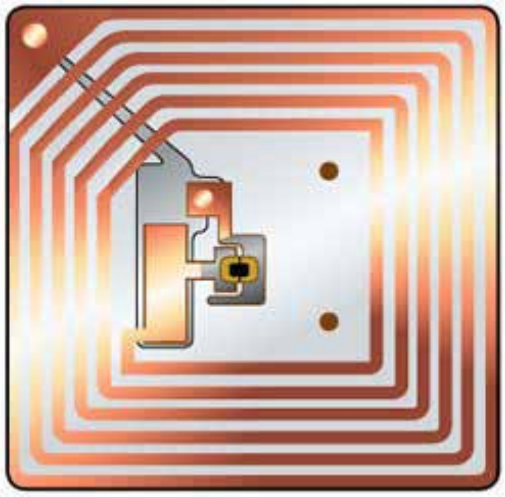

Figura 3

Esquema de un chip RFID (NFC, 2012). Apart (University, 2010).

Sistemas de identificación personal basados en biometría

Los sistemas de identificación de la actualidad se enrutan hacia la identificación de métricas que dependen de la biología humana; a estos sistemas se les conoce como sistemas de reconocimiento biométrico.

Los sistemas de reconocimiento biométrico pretenden empoderar las características y rasgos fisiológicos como elementos de identificación única, y estos han tenido un gran auge en tiempos recientes. La biometría ha probado ser un factor certero, simple y eficaz en el reconocimiento de los individuos; el reconocimiento fisiológico se basa en características corporales

que son prácticamente imposibles de replicar. El reconocimiento biométrico se especializa en el reconocimiento de:

Huellas dactilares.
Palma de la mano.
Retina.
Caracterización de rasgos del rostro

Entre las innovaciones que se pueden encontrar en el reconocimiento basado en biometría encontramos las combinaciones entre sistemas de reconocimiento de rasgos, los sistemas de sensores de señales fisiológicas y los sistemas de reconocimiento de gesticulación.

Anteriormente los sistemas basados en biometría podrían ser simples y eficientes, pero cuando en un sistema, además de reconocer las características de una huella digital, se analizan cosas como la temperatura y humedad del dedo, la forma de posicionarlo, el volumen de pigmentación de la piel, los horarios de reconocimiento y los usos horarios, la geolocalización y la fuerza de contacto, es más complicado replicar una muestra; estos son ejemplos claros del robustecimiento de los sistemas biométricos y su especialización en el reconocimiento de un ente dentro del sistema.

Otro ejemplo del avance en la biometría sería los sistemas modernos de reconocimiento facial. Dentro de los primeros sistemas desarrollados se establecían parámetros de métricas entre los rasgos faciales, los cuales podrían ser replicados con una imagen fotográfica, pero en sistemas más recientes la captura y métrica son solo el primer elemento; los sistemas de reconocimiento por imagen reconocen ahora también la gesticulación cotidiana de los usuarios, así como el avance progresivo de las características fisiológicas del individuo. Así pues ahora no basta con reconocer la imagen, también se reconocen particularidades como la sonrisa, el parpadeo, el crecimiento de vello facial, la aparición de cicatrices entre muchas otras.

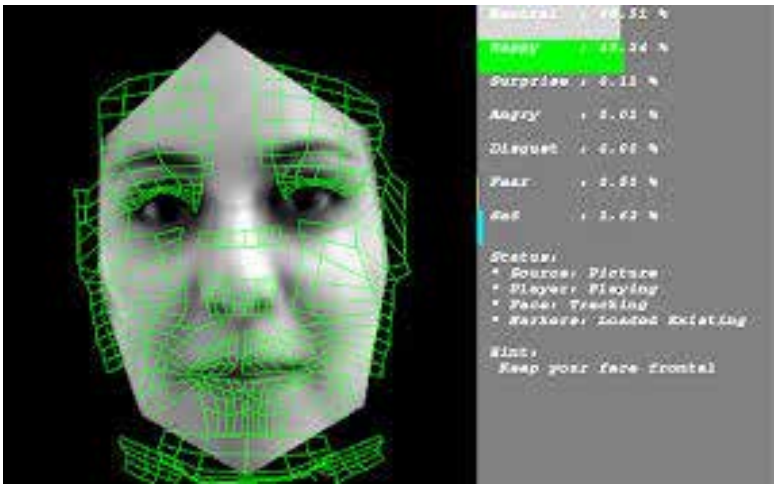

Figura 4

Reconocimiento facial basado en el reconocimiento de gesticulación (Neurmarca, 2011). sitio Hotmail (Acunetix, 2015).

Finalmente tendencias de reconocimiento biométrico pretenden en un futuro no muy lejano el reconocimiento de rasgos biológicos más especializados y complejos como el genoma humano. En sus principios, el reconocimiento de las cadenas de ADN tardaba meses basados en las técnicas iniciales; en la

actualidad se pueden tener resultados confiables en un promedio de entre 1 día y unas cuantas horas.

Existen trabajos de investigación más recientes que tiene como objetivo el reconocimiento de cadenas superiores de ADN en un tiempo más corto y que basado en estas se pueda realizar un reconocimiento personal de un individuo con una simple muestra de sudor, saliva o vaho, por lo que se prevé que existan sistemas que nos puedan reconocer simplemente empañando un cristal con el vaho de la boca.

La implementación de sistemas de reconocimiento personal es una tendencia dentro del área tecnológica, por lo que es importante reconocer ciertos parámetros para la elección de la mejor opción:

El costo del sistema.
El nivel de seguridad.
El acceso a la infraestructura.
El objetivo del sistema
El alcance y escalabilidad del sistema de comunicación y el sistema de información

La implementación de sistemas de identificación se debe realizar preferiblemente en coordinación con un equipo que debe estar integrado por especialistas de seguridad, departamentos de sistemas y de informática, muestras de los usuarios del sistema y dirección y planeación de la institucion que pretende la implementación.

Dentro de las tendencias de sistemas de seguridad y de identificación personal se encuentras empresas que sirven como punto de referencia y que dan sus perspectivas sobre el progreso de la tecnología como HID Global, la cual ha marcado las expectativas en los sistemas de identificación y avances tecnológicos y así presenta informes sobre dichas tendencias como:

“HID Global®, líder mundial en soluciones confiables de identificación, prevé un cambio en el uso de la tecnología de identificación que llevará a una mayor adopción de dispositivos móviles y de la última tecnología de tarjetas inteligentes, a una mayor importancia y dependencia de la nube, y a una forma radicalmente nueva de concebir la confiabilidad en entornos inteligentes y del Internet de las cosas (IoT) (Global, 2017)”.

Resultados, conclusiones y trabajos futuros

La aportación que dan los sistemas de identificación personal al mundo de la informática es remarcable y debe ser considerada en la creación de sistemas modernos en los que según las tendencias se pretende compartir información a través de la nube, que esta información esté disponible bajo cualquier medio de acceso móvil y sistemas de reconocimiento inteligente y que dicha información pueda ser utilizada en la toma de decisiones o en la adecuación de nuestra realidad con sistemas que puedan ser accesibles al internet de las cosas (IoT).

Basado en el análisis de las tendencias de sistemas información se puede concluir que la elección de estos se debe basar principalmente en las necesidades de seguridad, la infraestructura tecnológica disponible y en las características de información personal necesarias a reconocer.

La identificación en sistemas informáticos asado en la entrega de credenciales es una tendencia en sistemas de información; su implementación es simple y su facultad de seguridad depende de las destrezas de los desarrolladores que crean el proyecto; aunque su flexibilidad es importante, éstos no son recomendados para su uso en sistemas automatizados, puesto que son propensos a mayos disposición de tiempo en su identificación y en la utopía de los sistemas automáticos, pueden provocar errores en la escritura que generan desviación del objetivo primordial de los sistemas aquí descritos la cual se basa en un uso simple, rápido y eficiente.

Los sistemas biométricos son considerados los más útiles en el reconocimiento personal cuando las características de seguridad requieren un alto nivel de confiabilidad, teniendo en consideración que un sistema biométrico combinado (que analiza más de un solo rasgo biométrico, como retina y dactilar juntos), aunque su inconveniente es el costo y la infraestructura tecnológica a habilitar, así como los recursos de sistemas de información implícitos para el manejo de los datos digitales generados por éstos.

Los sistemas de identificación por tags personales son una opción adecuada para los sistemas automatizados que necesitan una validación de usuarios y que no requieren grandes medidas de seguridad, esto basado en el costo de su implementación, la fiabilidad de su identificación, y la regeneración de tags y la durabilidad del mismo.

Figura 5

Comparativa de sistemas de identificación personal (propio del autor).
gesticulación (Neurmarca, 2011).
sitio Hotmail (Acunetix, 2015).

Creación de sistemas automatizados basados en RFID

Los sistemas basados en la implementación de tags RFID suelen ser preferidos por el bajo costo y la eficiencia en los procesos de identificación, así como la durabilidad del mismo. Estos sistemas necesitan una infraestructura simple en la que se contemplan interfaces de comunicación sin requerimientos especializados más allá de los lectores y escritores de tarjetas y los simples tags que van a ser reconocidos en el mismo.

La tecnología RFID ha venido decreciendo en costo y todo lo contrario en accesibilidad y confiabilidad. Los sistemas RFID suelen ser compactos, económicos y simples, cumpliendo con los objetivos esenciales de estos: la identificación personal.

Figura 6

Estructura del sistema de identificación de usuarios basado en RFID.

Sistema de automatizados basados en RFID

Existen sistemas de identificación personal que pretenden la automatización de operaciones rutinarias en instituciones. En este caso ya no solo los el administrador podrá realizar varias tareas como:

Compra de servicios.
Instalación de citas.
Consulta de saldo e información personal de usuarios.
Consulta de servicios adquiridos y pendientes por atender.
Registro y actualización de servicios disponibles.
Revisión de historial de atenciones.
Registro de atención de servicios, entre otros

Los sistemas automatizados suelen tener una base en un sistema de identificación personal, por lo que los sistemas RFID son una gran oportunidad para crear un sistema integrado simple y compacto. Los kioscos electrónicos suelen ser una gran prestación para los usuarios y permiten que los sistemas que puedan ser autos administrados suelan ser más comunes y pertinentes a sus usuarios. Las tareas de procesos simples en los que los usuarios puedan manejar su propia información y realizar tareas de control de sus propias operaciones son una realidad al día de hoy y el reto para los fabricantes de software y desarrolladores se centra en la creación de ambientes amigables intuitivos, simples y funcionales que pretendan ofrecer este tipo de servicios.

Referencias

Acunetix, 2015. *Statistics from 10,000 leaked Hotmail passwords*. [En línea] Available at: https://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/ [Último acceso: 26 11 2017].

Bateman, J., Cortés, C., Cruz, P. & Paz-Penagos, H., 2009. Diseño de un protocolo de identificación por radiofrecuencia (RFID) propietario para una aplicación. *Sistema de Información Científica Redalyc Journal of Technology Management & Innovation*, pp. 325-339.

Botero D., J., González, D. & Paz, H., 2009. La interferencia como un factor que afecta el desempeño de un sistema RFID. *Sistema de Información Científica Redalyc Journal of Technology Management & Innovation*, pp. 145-153.

Global, H., 2017. HID *Global Powering Trusted Identities*. [En línea] Available at: https://www.hidglobal.mx/node/28062 [Último acceso: 27 11 2017].

N10, P., 2017. *Implante de chip está transformando pesonas en ciborgs*. [En línea] Available at: http://oportaln10.com.br/implante-de-chip-esta-transformando-pessoas-em-ciborgues-47508/ [Último acceso: 2 Junio 2017].

Neurmarca, 2011. *Software de reconocimiento de emociones a través expresiones faciales*. [En línea] Available at: http://neuromarca.com/blog/reconocimiento-facial-emociones/ [Último acceso: 26 11 2017].

NFC, M., 2012. *Diferencia entre NFC y RFID*. [En línea] Available at: https://mundonfc.wordpress.com/2012/02/08/diferencia-entre-nfc-y-rfid/ [Último acceso: 26 11 2017].

Pressman, R. S., 2006. Ingeniería de software, un enfoque práctico. México: McGrawHill.

Ramírez, J. J., 2012. Radio frequency identification (RFID) technology for academic, logistics and passenger transport. *Sistema de Información Científica Redalyc Journal of Technology Management & Innovation*, pp. 58-65.

SA, P. f., 2017. *Tecnología RFID, identificación automática por radiofrecuencia.* [En línea] Available at: http://www.puntoflotante.net/RFIDTUT.htm [Último acceso: 2 Junio 2017].

Seguridad, I., 2017. *Tag de largo alcance.* [En línea] Available at: http://www.iceseguridad.com/sis_tag.htm [Último acceso: 2 Junio 2017].

Sparkfun, 2014. *RFID Basics*. [En línea] Available at: https://learn.sparkfun.com/tutorials/rfid-basics [Último acceso: 2 Junio 2017].

Spychips, 2007. *RFID Journal Calls VeriChip Implant "unnecessary and a little creepy"*. [En línea] Available at: http://www.spychips.com/blog/verichip/ [Último acceso: 2 junio 2017].

University, C. M., 2010. *CAPTCHA*. [En línea] Available at: http://www.captcha.net/ [Último acceso: 25 11 2017].

Van de Wijngaert, L., Versendaal, J. & Matla, R., 2008. Business IT Alignment and technology adoption; The case of RFID in the logistics domain. *Sistema de Información Científica Redalyc Journal of Technology Management & Innovation*, pp. 71-80.

Veeramani, D., Tang, J. & Gutierrez, A., 2008. A Framework for Assessing the Value of RFID Implementation by Tier-One Suppliers to Major. *Sistema de Información Científica Redalyc Journal of Technology Management & Innovation*, pp. 55-70.

Wen, L., Zailani, S. & Fernando, Y., 2009. Determinants of RFID Adoption in Supply Chain among Manufacturing Companies in China: A. *Sistema de Información Científica Redalyc Journal of Technology Management & Innovation*, pp. 22-32.

Zetter, K., 2009. *Wired.com*. [En línea] Available at: https://www.wired.com/2009/10/10000-passwords/ [Último acceso: 25 11 2017].