Universidad Nacional de Costa Rica

Aplicaciones Globales Informáticas

Sistemas biométricos y sus implicaciones en la seguridad digital

Estefanía Murillo Romero 117000387

Julio Rodríguez Chavarría 116760031

2019

Resumen

Los sistemas biométricos son una ciencia y tecnología que analiza las características del cuerpo humano como herramienta para la autenticación e identificación de las personas. También, algunos de ellos van con un nuevo enfoque donde se analizan comportamientos de una persona. Estos mecanismos son una forma segura, ya que no hay forma de que sean olvidados, robados o suplantados. En la actualidad existen muchos mecanismos biométricos que tienen un rango muy amplio de confiabilidad. Estos sistemas se utilizan desde instalaciones de alta seguridad hasta aplicaciones muy básicas como desbloquear un teléfono inteligente.

Introducción

La seguridad de los datos e información es la principal preocupación de las empresas y entidades del presente. Al existir personas sin escrúpulos que se dedican al robo y apropiación de activos intangibles ajenos es que hay distintos métodos para salvaguardar la integridad y confidencialidad de estos. Métodos como contraseñas y pines quedaron obsoletos desde hace algún tiempo y por eso se debe de ir migrando hacia otras tecnologías que permitan mantener nuestros activos más valiosos a salvo. Los sistemas biométricos se han ido implementando poco a poco como una alternativa segura en esta era tecnológica. La biometría proporciona la verificación e identificación de los seres humanos por medio de patrones únicos, unos tipos son más seguros que otros pero sin lugar a dudas estas técnicas relativamente nuevas son la mejor opción para la seguridad digital.

El siguiente trabajo de investigación describe los conceptos básicos y diferentes tipos de sistemas biométricos que se utilizan en la actualidad para complementar la seguridad digital.

Metodología

Para la extracción de información del presente artículo se hizo uso de la base de datos de la Universidad Nacional, la herramienta Google Académico y distintas páginas web informativas. Se analizaron y revisaron múltiples artículos y sitios web con información relevante para el mismo. Se escogieron las mejores fuentes para aportar un trabajo sustancioso.

Desarrollo y discusión

Bios quiere decir vida y metría medida [11], por lo que un sistema biométrico es un sistema tecnológico capaz de analizar la información de una persona u organismo biológico y poder autenticar o identificar a este. Estos sistemas dependen de la recolección de datos únicos en cada persona para funcionar efectivamente [12].

La seguridad digital se define como un conjunto de acciones con el propósito de proteger elementos computacionales y de telecomunicaciones contra amenazas y riesgos que comprometan la confidencialidad, integridad y disponibilidad de los mismos. [9]

Estos sistemas tienen dos enfoques, la verificación e identificación. “La verificación permite autenticar la identidad de la persona comparando los registros en la base de datos con los que se acaban de obtener. La identificación reconoce al usuario mediante el rasgo de la base de datos que se asemeje al mismo.” [11]

Actualmente, los gobiernos y compañías tecnológicas han mostrado interés en el desarrollo de estas tecnologías para diversos propósitos que van desde la seguridad de la información hasta el reconocimiento de individuos específicos. [6]

Como se sabe, hoy en día la información es el activo más importante en nuestra sociedad y la seguridad de esto siempre ha sido una incertidumbre. Los sistemas biométricos han venido a cambiar la forma en la que se obtiene la información de diferentes entidades y le brinda una solución a esa incertidumbre. Es por eso que actualmente existen muchos sistemas biométricos que se han ido incorporando en

los diferentes sectores del mercado con el fin de proporcionar una mejor experiencia de usuario en cuanto a la seguridad digital. Los distintos sistemas biométricos se pueden clasificar como estáticos y dinámicos. Los sistemas estáticos son los sistemas que incluyen un reconocimiento físico del ser humano y los dinámicos se refieren a reconocimientos a partir de características conductuales. [12] Entre los estáticos se encuentran los siguientes:

- Reconocimiento facial: Es uno de los sistemas biométricos más utilizados por la industria por ser una interacción común entre las personas. También es un método no intrusivo, es decir con solo una cámara es posible detectarlo. [11] Además, por medio de esta técnica es posible reconocer el estado de ánimo de la persona. Como desventaja, este método no podría acertar totalmente en caso de cambios en el rostro (como barba, lentes, alguna lesión) [10] ni tampoco logra diferenciar del todo a las personas idénticas como gemelos o mellizos.
- Termograma facial: Es el reconocimiento por medio de una cámara térmica. [11] “Mide los patrones infrarrojos de emisión de la cara producidos por el flujo de sangre bajo la piel. [12]” Para esta técnica no afectan los cambios en el rostro como sucede con el reconocimiento facial, sin embargo presenta la desventaja de que sí afecta si la persona tiene una gripe o si viene de realizar ejercicios. [11] Se puede escanear a unos cuantos metros de distancia. [12]
- Labios: Los labios se pueden identificar por medio del movimiento, la huella y la forma. [12] La huella es única en cada persona, la forma ayuda como una característica para identificar a la persona y el movimiento ayuda a través del reconocimiento de voz. [12]
- Oreja: Esta técnica es bastante confiable ya que no es un elemento que esté en constante cambio y se maneja de igual manera que la huella digital. El problema es que muchas veces las personas ocultan las orejas con el cabello, algún sombrero [11], por condición de salud o de religión. Para poder ser captada correctamente es necesario descubrirla ante una cámara. [10]
- Ojo: Para el ojo es posible dos reconocimientos: el iris y la retina.

    - Iris: Se dice que es característico para cada humano. Se puede obtener fácilmente con colaboración del usuario pero también hay mecanismos que permiten obtener la imagen sin la colaboración.[11] Se cree que es una de las mejores técnicas, ya que se mantiene de la misma forma toda la vida por la protección que le brinda la córnea. [10]
    - Retina: Es una técnica de baja aceptación. Se trata de leer las venas que hay dentro de la retina con una luz infrarroja. [11]
- Mano: Para esta técnica se mide el largo y ancho de los dedos y el ancho de la mano, se cree que es un rasgo que no cambia. Para tomar esta técnica es necesario que el usuario coopere. [11] Es bastante aceptada por el usuario. [10] Se utiliza comúnmente en sistemas que tengan almacenamiento limitado ya que los requerimientos del mismo no son muchos.[11]
- Huella dactilar: Esta técnica ha sido la más estudiada y utilizada durante años, se ha logrado probar que cada humano presenta huellas únicas y que se mantienen estables a lo largo del tiempo. [10] Esta tecnología es bastante aceptada por los usuarios, es de las más baratas de implementar y es utilizada en aplicaciones forenses, civiles y de seguridad. [11]
- Venas de la mano: Es la tecnología más reciente, esta técnica trata de leer la estructura de las venas de la mano por medio de una luz infrarroja. [11] Estas poseen múltiples características que las hacen únicas para cada ser humano. [10] Es más o menos aceptada por el usuario. En cuanto a seguridad compete, no es falsificable. [11]

Entre los dinámicos se destacan los siguientes:

- Firma: Es una técnica bastante aceptada durante mucho tiempo para trámites gubernamentales, administrativos entre otros. Sin embargo, no es una manera confiable para verificar la identidad de una persona ya que la firma y la forma de escribir de las personas puede variar con el tiempo debido a factores físicos y emocionales. Además, algunos profesionales pueden crear firmas similares y el ojo humano no sería capaz de identificar la real de la falsa. [11]
- Voz: Es una técnica poco segura porque algunas personas tienen la facilidad de imitar a otras por su voz, influye la salud de la persona que está siendo

verificada (dolor de garganta, enfermedad, estrés…) y también influye el la calidad del canal de comunicación (micrófono, sistema de digitalización) [11]

- Forma de teclear: Técnica para verificar si el individuo es o no. Examina la velocidad, ritmo, patrones durante el tecleo. [11] Se mantiene la hipótesis de que el ritmo mientras una persona escribe en una máquina es característico de ella. [10] Se utiliza normalmente como un programa oculto en la computadora de la persona y se verifica mediante redes neuronales, clasificadores bayesianos y sistemas difusos. [12]
- Forma de caminar: Se utiliza para identificar a una persona por medio de patrones mientras camina. [12] Se mide el ritmo, velocidad, la forma de los pasos, entre otros. Los algoritmos son capaces de extraer la silueta de la persona y analizar todos los factores anteriormente mencionados para la verificación de la misma. [11] Además, hay otro tipo de elementos que influyen en un resultado acertado, como lo son si la persona carga objetos con ella, si camina con agotamiento, entre otros. [11] Como ventaja es que puede utilizarse a la distancia sin que la persona se de cuenta. [12]

Dados los diferentes métodos que existen para verificación biométrica, el siguiente paso es lograr encontrar un método efectivo que ofrezca un alto nivel de adaptabilidad a la mayoría de los casos en que es aplicable la biometría. Uno de los mayores problemas que presentan los sistemas biométricos estáticos son las limitaciones que se pueden dar por depender de características específicas de los usuarios. Cada uno de estos sistemas resuelve la verificación de una manera distinta tomando en cuenta partes diferentes del cuerpo humano. A comparación con los sistemas anteriores, algunos de los dinámicos ofrecen un grado mayor de adaptabilidad por estar basados en redes neuronales que son capaces de entender los comportamientos de las personas y sus cambios. Un problema que puede presentar es que necesitan tiempo para conocer de manera precisa al usuario que se desea verificar y pueden ser aplicados a escenarios más específicos. Sin embargo, ningún método es mejor que otro, todo depende de la aplicación que se le dé.

Los diferentes sistemas biométricos pueden usarse mucho en distintas actividades cotidianas y emplearse en distintos sectores del mercado para garantizar mayor seguridad y confiabilidad en los procesos:

- Por ataques de phishing, ingeniería social, skimming, entre otros el sector bancario se encuentra realmente vulnerable. El uso de tarjetas, contraseñas o pines es un riesgo para el usuario y la entidad, ya que están expuestos a fraudes, pérdidas, robos. Es así como estas instituciones hacen uso de sistemas biométricos para proveer mecanismos más seguros y complejos para quién quiera cometer acciones fraudulentas. [4] BBVA Bancomer, entidad bancaria, brinda un servicio llamado *Alta inmediata* que permite a sus clientes crearse una cuenta con el celular, como requisito únicamente tomarse una foto y responder una llamada de voz; esto con el fin de tomar su voz y rostro para la autenticación la próxima vez que ingrese. [3] BBVA Bancomer está haciendo uso de 3 técnicas biométricas para que la autenticación de sus clientes, las cuales son:
    - Huella dactilar. [8]
    - Voz: verifica que concuerden la frecuencia, acento y velocidad. [8]
    - Rostro: Verifica la distancia entre las pupilas, nariz y demás características del cliente. [8]
- Pagos electrónicos: Organizaciones como Visa, Banco Neon de Brasil, MasterCard con su servicios Identity Check, AliPay permiten agilizar los trámites de compras por medio del sistema biométrico de rostro. Esta innovación les da una mejor experiencia de usuario en cuanto a seguridad y rapidez de procesos. [2]
- Acceso a sus servicios: Empresas y tecnologías están haciendo uso de las huellas dactilares o reconocimientos faciales, tal es el caso de Disney, celulares, cajeros automáticos entre otros. [1]
- Identificación de los ciudadanos: El gobierno utiliza estos sistemas para identificar a cada uno de los que pertenecen a su región y a los migrantes. [1]

- Medicina: El reconocimiento de oreja es utilizado para la medicina legal y forense. [12] El reconocimiento vascular permite identificar a pacientes rápidamente y consultar su historial y datos médicos. [5]

Esta tecnología está teniendo mucho auge y aceptabilidad por parte de los usuarios. Es necesario que las compañías y tecnologías sigan implementándolas para bajar el riesgo de un ataque o robo cibernético.

Conclusiones

Actualmente vivimos en la era digital donde todos los días hay avances nuevos que lograr mejorar la calidad de vida de las personas. En esta nueva época además de existir nuevas oportunidades, también surgen nuevos retos con relación a la seguridad de la información y la manera que esta es accedida. Analizando la información presentada en esta investigación, se pueden ver beneficios claros para las personas y los gobiernos por la implementación de tecnologías que permitan garantizar el uso correcto de la información y su seguridad. Una vez estos nuevos enfoques logren ser implementados con una estabilidad suficiente para garantizar el funcionamiento y la confianza sobre la seguridad de los datos, se puede pensar en dejar atrás métodos comunes para la verificación de personas y la dependencia de contraseñas para acceder a la información.

Vistos lo puntos anteriores, se expuso sobre los métodos que actualmente han tenido una adopción considerable por la población. Por otra parte se habla sobre posibles direcciones que pueda tomar este tema en el futuro con la implementación de sistemas más sofisticados que no dependan de factores estáticos como lo son algunas de las características físicas de las personas, pero más bien basar su funcionamiento en procedimientos dinámicos como el comportamiento o patrones que pueden ser analizados por un algoritmo para entender mejor a un usuario.

Predecir qué dirección tomará este tema es un tema difícil de expresar pero sí es claro que es un área muy prometedora con un potencial totalmente capaz de cambiar la manera en que los datos son manipulados y saber a quién le pertenecen.

Referencias

[1] Acceso por Huella. (2018) Aplicaciones de la biometría en la vida cotidiana. Recuperado de: https://accesoporhuella.com/aplicaciones-biometria/

[2] Chacón, K. (2017) Banca da sus primeros pasos en el uso de la biometría para trámites. Recuperado de: https://www.nacion.com/economia/banca/banca-da-sus-primeros-pasos-en-el-uso-de-la-biometria-para-tramites/75GKPIUHDFDMLDOXN3SLLBVHYM/story/

[3] Communications. (2018) La biometría se abre paso en las finanzas personales. Recuperado de: https://docs.google.com/document/d/1By92B_tzia_N0tZdmKuc4uyzPjOYwJGbw2BKKghSFM0/edit#

[4] Equipo Editorial. (2019) El sector bancario y la seguridad biométrica. Recuperado de: https://reportedigital.com/seguridad/biometria-seguridad-digital-sector-bancario/

[5] García, I. [Umanick Technologies] (2017, febrero 24) ¿Cómo funciona un sistema biométrico? [Archivo de video] Recuperado de: https://www.youtube.com/watch?v=P2FEev3fWWY

[6] Mezgár, I. (2006). Trust in e-government services. In *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce* (pp. 1094-1100). IGI Global.

[7] Mishra, A. (2010). Multimodal biometrics it is: need for future systems. *International journal of computer applications*, *3*(4), 28-33. Recuperado de: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.3836&rep=rep1&type=pdf

[8] Peña, M. Silva, S. (2018) La incorporación de biométricos refuerza la seguridad de los clientes de BBVA Bancomer. Recuperado de: https://www.bbva.com/es/incorporacion-biometricos-refuerza-seguridad-clientes-bbva-bancomer/

[9] ¿Qué es la seguridad informática?. (s.f) Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=2ahUKEwjsl4X8ib7lAhXjQd8KHXVkA0oQFjAOegQICBAC&url=http%3A%2F%2Fwww.scm.oas.org%2Fidms_public%2FSPANISH%2Fhist_05%2Fcitel02548s02.doc&usg=AOvVaw2tzBJh_UadKNYYMcHGyuXp

[10] RUIZ MARÍN, M., RODRÍGUEZ URIBE, J., & OLIVARES MORALES, J. (2009). UNA MIRADA A LA BIOMETRÍA. *Avances en Sistemas e Informática, 6*(2), 29-38. Recuperado de https://revistas.unal.edu.co/index.php/avances/article/view/20295

[11] Serratosa, F. (2012). La biometría para la identificación de las personas. *Editorial UOC. España*.

[12] Suárez Hernández, D., & Herrera Luna, E. C. (2008). *La firma como un método biométrico de identificación*. Instituto Politécnico Nacional. Centro de Investigación en Computación. Recuperado de: http://repositoriodigital.ipn.mx/handle/123456789/8502

[13] Techopedia. (s.f). *What is a Biometric System?.* Retrieved from http://www.techopedia.com/definition/26990/biometric-system