Seguridad Biométrica

Isabel Galeano Hernández
lgaleanoh@ucenfotec.ac.cr

Universidad Cenfotec
Bachillerato en Ingeniería de Software

Abstract
Actualmente la tecnología se encuentra integrada en casi todos los aspectos cotidianos del ser humano y con la digitalización que sigue creciendo, se ha vuelto una tarea difícil proteger la información confidencial. Por ello, se ha planteado una nueva forma de seguridad al mundo, la seguridad biométrica.

Palabras Clave
Biométrico, seguridad, identificadores, huellas digitales, geometría facial, usuario, empresa.

Introducción

La seguridad biométrica es un mecanismo de seguridad que se encarga de identificar a las personas mediante verificación de sus características físicas o de comportamiento. Actualmente es utilizada en múltiples entornos, tales como; sistemas que almacenan huellas dactilares, patrones retinales, entre otros.

Desarrollo del tema

El objetivo de utilizar seguridad biométrica es proporcionar una técnica de seguridad física más sólida y precisa que se utilice para la verificación de identidad. La biometría es utilizada principalmente en sistemas de seguridad de entornos que están sujetos a robo o que tienen requisitos críticos de seguridad física. Estos sistemas almacenan las características que permanecen como constantes a lo largo del tiempo, es decir huellas dactilares, reconocimiento facial, voz, patrones manuales, entre otros. Estas características se almacenan que se mencionaron con anterioridad son como plantillas en el sistema. Es decir, cuando alguien intenta acceder al sistema, el sistema de seguridad biométrica lo escanea, evalúa las características e intenta compararlo con los registros almacenados. Después, si se encuentra una coincidencia, la persona tiene acceso a la instalación o dispositivo.

Identificadores Biométricos

Los identificadores biométricos hacen referencia a identificadores físicos únicos que utilizan los sistemas de reconocimiento automático. Por ejemplo, las venas de la palma de la mano, las huellas dactilares, la forma y el patrón del iris de los ojos, todos estos se consideran biométricos únicos.

Importancia de la seguridad biométrica

En el ámbito empresarial, las empresas pueden obtener beneficios de implementar sistemas de seguridad biométrica y obtener una seguridad sin precedentes de la información restringida. Huellas dactilares, patrones de iris y escaneos de retina, cuando se capturan de forma correcta, producen conjuntos de datos totalmente únicos. Además, la seguridad biométrica, puede proteger los activos de la empresa como las computadoras y activos comerciales. Y en

caso de ser empresas que trabajan de forma presencial, es crucial que personas no autorizadas no puedan acceder a redes y sistemas seguros.Asimismo, las empresas tienen reglas de cumplimiento que deben garantizar que solo ciertos empleados tengan acceso a archivos confidenciales Para datos confidenciales de suma importancia, las contraseñas no solventan los problemas, ya estas pueden compartirse entre compañeros de trabajo. En cambio, las organizaciones pueden usar la biometría para regular el acceso a servidores o computadoras.

Funcionamiento de los sistemas de seguridad biométricos

Luego de recopilar y comparar los datos biométricos de una persona, estos se guardan en el sistema para compararlos con intentos de acceso posteriores. Usualmente, los datos biométricos se cifran y luego se almacenan en el propio dispositivo o en un servidor remoto.
El hardware que se conoce como escáner biométrico captura las características físicas para la verificación y autenticación de la identidad. Los escaneos del hardware se comparan con la base de datos guardada y, dependiendo de si se encuentra una coincidencia, se otorga o restringe el acceso.

Tipos de seguridad biométrica

Actualmente existen dos tipos principales de seguridad biométrica, física y de comportamiento. La biometría física se encarga de analizarlos rasgos faciales, la estructura de los ojos, forma de la mano, es decir, lo relacionado con el cuerpo físico. Con la biometría del comportamiento, el sistema analiza cualquier patrón de comportamiento que se encuentre asociado con el individuo. Algunos ejemplos de seguridad biométrica física son; huellas dactilares, geometría facial, retina, iris, forma del cráneo, venas de las palmas o dedos, entre otras.
También, cabe destacar algunos ejemplos de seguridad biométrica de comportamiento; marcha, firma, reconocimiento del hablante, entre otros.

Riesgos de seguridad

Como se mencionó con anterioridad, las múltiples ventajas que proporciona la seguridad biométrica son muchas, pero, se debe tener en cuenta que no garantiza una ciberseguridad absoluta. Existen posibilidades de que la seguridad sea violada, Por ejemplo, los delincuentes pueden "levantar" las huellas dactilares de las superficies y utilizarlas para acceder a sistemas protegidos biométricamente. Otro ejemplo, es el robo de huellas dactilares, el cual no evita que se brindan accesos a lugares e información confidencial. También, es posible engañar la seguridad con tecnologías de reconocimiento facial, tales como modelos 3D de fotografías de rostros 2D.

Formas de proteger los datos biométricos

Existen formas en las que se puede asumir la responsabilidad personal de proteger los datos. Algunas pautas que las personas deben seguir para proteger su información biométrica personal son; Se debería compartir datos biométricos sólo con organizaciones altamente confiables. Asimismo, antes de compartir datos biométricos con organizaciones, hay que asegurarse de que tengan implementadas las medidas de ciberseguridad necesarias.

Y por último, utilizar contraseñas seguras para dificultar que se realicen robos de la información almacenada, además de utilizar un software de ciberseguridad acreditado para salvaguardar la información digital.
De acuerdo a lo anterior, alguna pautas que las empresas deberían seguir para aumentar la seguridad de estos sistemas son; Mantener todos los sistemas y software actualizados; Utilizar autenticación multifactor y contraseñas internas seguras; Poseer un software de seguridad cibernética sólido y de buena reputación; Utilizar tecnología anti-spoofing para proteger el sistema de infracciones.

Ventajas de la seguridad biométrica
La biometría es inherente al usuario. En la gran mayoría de los casos, aspectos físicos como las huellas dactilares nunca cambian. La biometría es difícil de duplicar. Permite un aumento de eficiencia, las personas pueden autenticarse en segundos, lo que reduce posibilidad de retrasos, tales como ingresar contraseñas. Proporciona la ventaja de adquirir menos personal de seguridad, lo cual significa que las empresas pueden ahorrar dinero ya que hay menos necesidad de asignar personal de seguridad dedicado a los puntos de acceso.

Desventajas de la seguridad biométrica
El entorno puede afectar la seguridad biométrica, tales como lugares muy fríos, Puede haber una falsa aceptación o un falso rechazo. Requieren hardware e integraciones muy costosas, además de que se requiere programadores para la administración del sistema.
Pueden ocurrir problemas de escaneo. Tales como personas que utilizan anteojos, si usa anteojos durante un escaneo del iris, esto podría causar dificultades. Los datos biométricos no se pueden establecer si están comprometidos. Es decir si hay un robo de huella dactilar, esta no puede cambiarse.

Conclusión
De acuerdo a todo lo mencionado con anterioridad, podemos concluir que la seguridad biométrica es una medida muy segura y recomendada a implementar por las empresas, siempre y cuando se tengan en cuentas sus ventajas y desventajas. Asimismo, el conocimiento de cómo mantener más seguros los datos biométricos.

Referencias

Kaspersky. (2022, 9 febrero). What is Biometrics? How is it used in security? Www.Kaspersky.Com. Recuperado 24 de junio de 2022, de https://www.kaspersky.com/resource-center/definitions/biometrics
Biometrics: definition, use cases, latest news. (2021, 9 noviembre). Thales Group. Recuperado 24 de junio de 2022, de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics
What Are Biometrics? The Pros/Cons of Biometric Security. (2021, 24 mayo). Auth0 - Blog. Recuperado 24 de junio de 2022, de https://auth0.com/blog/what-are-biometrics-the-proscons-of-biometric-security/
Gillis, A. S., Loshin, P., & Cobb, M. (2021, 26 julio). biometrics. SearchSecurity. Recuperado 24 de junio de 2022, de https://www.techtarget.com/searchsecurity/definition/biometrics