UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMATICA

TESIS DE GRADO

"IDENTIFICACION BIOMETRICA EN LA NUBE"

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN: INGENIERIA DE SISTEMAS INFORMÁTICOS

POSTULANTE: MAURICIO MATEO ALARCÓN CANEDO
TUTOR METODOLOGICO: M. Sc FRANZ CUEVAS QUIROZ
ASESOR: Lic. BRIGIDA CARVAJAL BLANCO

NUESTRA SEÑORA DE LA PAZ – BOLIVIA
2017

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

Dedicatoria

Dedicado a todos aquellos que buscan el conocimiento.

A todos aquellos que dan lo mejor de sí día a día.

A todos los que se esfuerzan por superarse.

A aquellos que nunca se rinden.

Y por supuesto a mi familia, que me enseñó a ser una de estas personas.

Agradecimientos

Mi más profundo agradecimiento a todas las personas que me apoyaron en la conclusión de este trabajo.

Al M.Sc. Franz Cuevas por la orientación y continuo apoyo brindado durante el desarrollo de esta tesis con su conocimiento y experiencia.

A la Lic. Brigida Carvajal por su constante disposición a ayudar a sus estudiantes y persistente ánimo de dar lo mejor de sí por su trabajo como docente.

A mi familia por su paciencia y apoyo.

A los administrativos por su constante ayuda y paciencia, en especial a Fernando, Daniel y Willy de Biblioteca y a Vanessa de dirección de carrera

Resumen

Los servicios en la nube son una opción conveniente para el procesamiento de datos tanto para individuos como para empresas. Los proveedores de servicios en la nube se encargan de las labores más complicadas de tener servidores, como el mantenimiento de los servidores, la redundancia de datos, la seguridad física y lógica, entre otros. Es así que los clientes tan solo se deben preocupar por la solución de sus propios problemas.

El acceso a los servicios en la nube es a través de una contraseña, o en algunos casos verificación telefónica. Sin embargo en los últimos años ocurrieron muchos incidentes que comprometieron datos importantes de empresas y personas que usaban los servicios en la nube. Esto provocó una desconfianza en el uso de esta conveniente herramienta. Es por eso que esta tesis propone una manera alternativa de acceder a los servicios en la nube. A través de la huella digital del cliente.

La tecnología de huella digital permite la identificación única y precisa de un individuo. Se plantea usar un dispositivo con acceso a internet e identificador de huella digital para acceder y realizar acciones en un sitio web de forma conveniente y segura.

Palabras clave: Nube, Arduino, Lector, Huella digital

Abstract

Cloud Services are a convenient alternative for data processing, both for people and enterprises. Cloud service providers take care of the most complicated tasks regarding server usage. As the maintenance of the servers, the data redundancy, the physical and logical security, amongst others. The idea is that clients only deal with solving their own problems.

A password is needed to access a cloud service, some cloud services even offer phone verification. Nevertheless, in recent years, many people and enterprises using cloud services reported their data to be compromised, where they lost their data or it was revealed. For this reason this thesis proposes an alternative to access cloud services. Through biometric identification.

The fingerprint allows a person's unique and precise identification. Using a fingerprint scanner to access cloud services in a convenient and secure way is the goal of this thesis.

Contenido

Índice de Figuras

CAPÍTULO I

MARCO REFERENCIAL

1.1. Introducción

Brindar servicios Web por internet requiere de servidores que reciban y procesen las solicitudes de los usuarios y realicen una variedad de operaciones. El mantenimiento de estos servidores es costoso ya que se debe pagar continuamente por la ventilación, la electricidad, el mantenimiento y reparación de los equipos, la seguridad física y el alojamiento en un data center. Todo esto sin tomar en cuenta el costo inicial de los servidores. Es por todo esto que ahora existen proveedores que se encargan de todos estos aspectos, llamados proveedores de servicios en la nube, y venden el uso de sus servidores por periodos de tiempo o consumo de datos a múltiples clientes. Estos clientes pagan un monto de dinero por el uso de los servidores y ya no es tan costoso, primero porque son varios los clientes que pagan por los servidores y segundo porque tan solo utilizan tanto poder de procesamiento y almacenamiento de los servidores como necesitan.

El proveedor de servicios en la nube es el que tiene los servidores físicamente. Es por ello que el cliente tan solo puede acceder a sus aplicaciones a través de Internet. Usualmente al cliente se le brinda una contraseña con la que puede ingresar y realizar operaciones. Este cliente puede tener a la vez muchos usuarios en su aplicación web los cuales también tienen contraseñas y pueden modificar la aplicación de alguna manera. Si un intruso llega a obtener una contraseña

de un administrador o alguien con privilegios en la aplicación web, puede provocar pérdidas de información de gran magnitud. Y esto sumado al hecho de que no se tiene acceso físico a los servidores hace más atractivo el ataque a este servicio web.

Muchas empresas identifican este tipo de preocupaciones por la seguridad como la principal razón por la que no optan por utilizar servicios en la nube más activamente y beneficiarse de los costos reducidos que ofrece la nube (Genes, 2011). Y con buena razón puesto que muchas de estas empresas necesitan procesar datos que son delicados e inclusive secretos, que no quieren compartir con competidores u otras empresas, y cuya vulneración puede provocar pérdidas de cantidades significativas de dinero.

La contraseña es tan solo un solo factor para la identificación del usuario. Otros factores de identificación deben ser tomados en cuenta. Esta tesis propone el uso de tres factores para la correcta identificación del usuario. La contraseña, un dispositivo que posea el usuario y su huella digital.

1.2. Antecedentes

1.2.1. Identificación de dos factores de Google y Amazon

Tanto los servicios en la nube de Google como los de Amazon, cuentan con una opción de identificación doble, llamada también identificación de dos factores (Cipriani, 2015). El primer factor es la contraseña del usuario y el segundo factor es un código de seguridad que se manda al celular del usuario para verificar en la aplicación en la nube, el usuario escribe el código en la aplicación y entonces puede ingresar.

Este mecanismo de identificación de dos factores se basa en la comprobación de dos factores importantes de un usuario, algo que conoce y algo que tiene. En este caso lo que conoce es la clave y lo que tiene es el dispositivo que posee. Esta doble capa de protección pretende proteger la información de intrusos que logran obtener la contraseña de algún usuario del sistema.

1.2.2. Identificación biométrica por reconocimiento de voz

Uno de los problemas con la identificación por contraseña de los proveedores de servicios en la nube, es que la misma reasignación de contraseña se hace vía correo electrónico y el mismo correo electrónico es vulnerable a los mismos ataques que el servicio en la nube. Es por eso que

Vallabhu Himabindu propone un modelo de identificación de usuario mediante la voz para servicios en la nube (Vallabhu, 2012).

Este modelo se basa en biometría de comportamiento, que es la identificación de patrones de los usuarios, como por ejemplo la forma de escribir o la voz. Según Vallabhu la combinación de estos métodos de identificación permite identificar únicamente a una persona y por tanto asegurar el acceso a la nube solo a las personas que deben ingresar.

1.3. Planteamiento del problema

La contraseña en un servicio de la nube representa en la mayoría de los casos toda la seguridad de la aplicación en la nube. Es decir el robo de identidad del usuario indicado puede tener graves consecuencias.

En el año 2014, Code Spaces, una empresa que proporcionaba una plataforma de servicios de colaboración de software tuvo que cerrar por un atacante que eliminó la información de la empresa y todos sus respaldos (Venezia, 2014). Un individuo logro conseguir la contraseña de uno de los administradores. Una vez dentro del sistema, amenazó con borrar información importante de la empresa si no se le entregaba dinero. Justo cuando la empresa iba a recuperar el control, el individuo borro gran parte de la información y provoco el eventual cierre de la empresa.

En el año 2014, JP Morgan Chase, una empresa financiera de los Estados Unidos, sufrió un ataque a su servicio de la nube porque una de las cuentas no requería doble factor de identificación (Leyden, 2014). Un individuo aprovecho esta brecha de seguridad e ingresó. Copió toda la información privada de los clientes de JP Morgan Chase y la hizo pública. Esta era la información privada de 83 millones de personas, y fue un factor que redujo enormemente la confiabilidad de la empresa.

Lamentablemente, estos son tan solo algunos de los casos de empresas que sufrieron pérdidas significativas por este problema. En un estudio realizado por la organización llamada Information is Beautiful, se tomó en cuenta todas las empresas que sufrieron pérdidas significativas de información (de más de 30.000 registros) de la última década. Este estudio incluía un total de 220 empresas, siendo mayor el número de empresas involucradas en los últimos 5 años. Según este estudio, el 60 por ciento de estos casos se debieron a algún tipo de

hacking (Quick, Hollowood, Miles, & Hampson, 2016). El resto de casos, se debían a errores de configuración, perdida de una computadora, publicaciones accidentales y niveles de seguridad muy pobres.

Linkedin, el mayor sitio de contactos profesionales, el cual tiene 175 millones de usuarios reporto que su base de datos de contraseñas fue vulnerada, ocasionada por una brecha de seguridad. Aproximadamente 6.5 millones de contraseñas fueron robadas y publicadas en foros rusos y más de 200,000 de estas contraseñas fueron desencriptadas (Silveira, 2012).

Pero no son solo las empresas las víctimas de estos ataques, también los gobiernos del mundo que utilizan servicios en la nube. Según The Breach Level Index, una organización dedicada a la recolección de datos relacionados al robo de registros de empresas y gobiernos, el robo de información gubernamental, el 2015 a nivel mundial llego a 300 billones de registros ocasionados por 272 ataques informáticos (Gertz, 2015). Lo cual significa un crecimiento de 474 por ciento respecto al 2014.

De acuerdo al estudio realizado por CSA (Cloud Security Alliance), de los 130 incidentes de este estudio el 40 por ciento de incidentes son uno de dos, el robo de identidad o la pérdida o robo de información (Cloud Security Alliance, 2013).

El robo de identidad de un usuario se refiere a la recuperación de los credenciales de dicho usuario. Estos credenciales los utiliza para ingresar al sistema y una vez recuperados por un tercero, éste puede ingresar como si fuera el usuario. Cada sistema tiene diferentes tipos de credenciales, siendo la más común, la contraseña.

La pérdida o robo de información se refiere al robo de información de los usuarios pero en otros sitios o aplicaciones web. Estos sitios web no suelen tener los niveles de seguridad adecuados, e individuos maliciosos pueden aprovecharse de esto. Esta información robada de otros sitios web puede ser usada para acceder a la cuenta del usuario en sitios más seguros.

Vulnerabilidad a técnicas de ingeniería social

Uno de los principales medios por los cuales se puede obtener una contraseña es a través de técnicas de ingeniería social.

De acuerdo al libro Fundamentos de la Ingeniería Social (Granger, 2001), la ingeniería social es una inteligente manipulación de la tendencia natural humana a la confianza. El objetivo de un

hacker que usa ingeniería social es obtener información que le permitirá acceso no autorizado a un sistema que procesa información valiosa a través de engaños o induciendo a un usuario legitimo a realizar una acción sospechosa.

En el caso de la nube, todo lo que se necesita es la clave y la contraseña y en algunos casos el dispositivo del individuo en cuestión.

La integridad y confidencialidad de la información basada en la nube es vulnerable al robo de identidad de los usuarios a través de técnicas de ingeniería social.

Mal uso de contraseñas

Las contraseñas por si mismas no son una mala idea. El problema es que las personas que las usan no saben usarlas adecuadamente. Lamentablemente a pesar de todos los esfuerzos que se hace por educar a la gente en el correcto uso de contraseñas, los resultados siguen siendo negativos.

Según un estudio realizado por Cloud Industry Forum de ataques a gran escala realizados a empresas grandes como Sony o Linkedin, se comprobó que más del 50 por ciento de las contraseñas de estos usuarios tiene menos de 8 caracteres, 50 por ciento tienen solo números o solo caracteres y menos del 1 por ciento tienen caracteres que no son alfanuméricos. Y por lo menos el 70 por ciento de estas contraseñas son susceptibles a ataques de búsqueda completa (Walters, 2016).

Otro problema es que los usuarios reúsan sus contraseñas en múltiples ocasiones. Según un estudio realizado por Ofcom, el comité de vigilancia en telecomunicaciones del Reino Unido, de 1805 adultos entre 16 y 25 años, se descubrió que el 55 por ciento de ellos usaba la misma contraseña para la mayoría de los sitios que visitaba (Cluley, 2013). El 26 por ciento de ellos usaban contraseñas fáciles, como cumpleaños o nombres de sus mascotas.

Este problema es aún mayor con el robo de información de sitios no seguros. Por ejemplo una persona que usa la misma contraseña en múltiples sitios web, puede dejar su contraseña en un sitio no seguro. Luego de un tiempo un individuo malicioso puede extraer esta información de ese sitio no seguro y usarla en un lugar más importante como una cuenta bancaria o de una empresa.

Los usuarios no usan el factor de identificación de contraseña adecuadamente.

Ataques internos

Si bien es cierto que se registra la actividad de todas las cuentas en los servicios de la nube, varias personas internas a la empresa tienen acceso a información delicada. Si la personas decide vender la información que tiene o su misma contraseña, puede alegar luego que su cuenta fue vulnerada y no hay un método que pueda distinguir si fue realmente esta persona la que hizo esta actividad maliciosa.

No se puede probar que una determinada persona fue la que realmente ingreso al sistema.

Todos estos incidentes tienen en común la extracción de credenciales del usuario para acceso no autorizado a la nube, esto se agrava más ya que la nube no tiene un lugar físico y toda operación (incluso las más cruciales) son llevadas a cabo desde cualquier lugar con internet. Es por esto que el problema a resolverse es el siguiente.

Las aplicaciones soportadas en la nube son vulnerables al robo de identidad de sus usuarios a través de la recuperación de una contraseña y al eventual riesgo de pérdida de su información.

1.4. Definición de objetivos

1.4.1. Objetivo general

Existen tres factores de identificación, algo que sabe el usuario, algo que tiene y algo que es. En este caso se plantea que estos tres factores sean, la contraseña, un dispositivo y la huella digital del usuario.

Implementar un servicio biométrico en la nube de triple factor de identificación, contraseña, dispositivo y huella digital para la identificación única de usuarios.

1.4.2. Objetivos específicos

Dispositivo de huella digital

El dispositivo de huella digital usado en este trabajo podrá conectarse a Internet ya sea por un puerto RJ45 o por una red Wifi. Una vez conectado el usuario podrá registrar su huella digital para realizar una acción, como por ejemplo la cancelación de un proceso, la eliminación de información o cualquier acción que en malas manos pueda ocasionar perdida de información valiosa.

Construir un dispositivo de reconocimiento de huella digital para la identificación de usuarios del servicio en la nube.

Elaboración de un servicio RESTful API

Para que el dispositivo pueda conectarse a la nube es necesario crear un servicio Web que permita al dispositivo comunicarse con el servidor en la nube. En este caso se hace uso de una interfaz de programa llamada RESTful API que permite la comunicación a través del protocolo HTTP.

Elaborar un servicio RESTful API para la comunicación con dispositivos de huella digital.

Proceso de identificación de huella digital

El proceso por el cual el usuario se identificara con el dispositivo de huella digital debe ser simple y seguro. Este proceso debe estar soportado por la parte Back-End de la aplicación con un sólido registro de permisos y nuevos usuarios.

Elaborar un proceso de identificación de huella digital para el acceso a los servicios de la nube.

1.5. Hipótesis

El servicio de identificación biométrica en la nube identifica al usuario de manera conveniente y segura.

1.6. Justificación

Uno de los más grandes beneficios de las aplicaciones basadas en la nube, es la cantidad de dinero que se deja de invertir en mantenimiento de servidores, seguridad física y redundancia de datos. En vez de esto se paga un solo monto mensual que en la mayoría de los casos es mucho más conveniente y se puede descontinuar a pedido.

La desventaja de la nube es la seguridad de la información que reside en ella. Esta tesis intenta tomar las ventajas de la nube (especialmente la económica) y resolver las desventajas en seguridad a través de la verificación de tres factores.

Hoy en día, la gente se acostumbra más y más a la identificación biometrica. No solo se la ve en bancos, oficinas y empresas, sino también en nuestros mismos celulares y laptops. La identificación biométrica para servicios en la nube es tan solo un paso más de este desarrollo.

Esta tecnología permitirá potencialmente que más empresas y negocios incurran en la nube y asimismo acercaran más a la gente a esta tecnología.

La verificación de tres factores comprende el factor biométrico como medida adicional de seguridad a aplicaciones en la nube. Esto permite que aplicaciones que procesan información delicada puedan utilizar las ventajas de la nube.

La biometría digital tiene varias ventajas como ser el hecho de que la huella digital no puede ser adivinada o robada, se queda con el usuario de por vida y es única. Es conveniente y puede escalar fácilmente junto a las aplicaciones que las usan. La precisión de estos dispositivos es alta y esto hace a la biometría digital una opción muy atractiva para empresas que quieren proteger sus datos.

Por otro lado esta tecnología ofrecida como servicio permite a personas que necesitan este tipo de seguridad un acceso más fácil a ésta. Tal como se ofrece servicios de predicción del clima también se podrá ofrecer servicios de identificación biométrica.

1.7. Alcances y limites

1.7.1. Alcances

Se armará un dispositivo electrónico de identificación de huella digital. En esencia se tienen los siguientes dispositivos:

- Arduino
- Dispositivo de huella digital
- Dispositivo de comunicación Wifi

Este dispositivo se conectara directamente con la nube, la cual tendrá consigo solicitudes de acciones a realizar que el dispositivo de huella digital permitirá o no dependiendo si la identificación es exitosa.

1.7.2. Limites

- El dispositivo de huella digital funciona con una conexión activa de internet que es configurada por línea de comandos
- El back-end del proyecto está diseñado para trabajar con varios dispositivos, sin embargo cada dispositivo tendría su propio registro de la huella de cada usuario

El presente trabajo aborda tan solo uno de las muchas verificaciones biométricas que existen, existe verificación por iris, por retina, por voz, facial, etc. Este tercer factor de identificación podría ser cualquier de ellas y quizás en casos particulares unas sean mejores que otras.

CAPÍTULO 2

MARCO TEORICO

2.1. Computación en la nube

La computación en la nube es un modelo para la habilitación de acceso conveniente, escalable y seguro a un conjunto de recursos computacionales configurables (ej. Redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y controlados con un mínimo esfuerzo o casi ninguna intervención del proveedor (Buyya, Vecchiola, & Selvi, Mastering Cloud Computing, 2013).

2.1.1. La nube como servicio

Desde la perspectiva del usuario, los servicios en la nube funcionan tal y como los servicios de agua o luz del hogar. Esto quiere decir que el usuario usa el servicio tanto como necesita y no debe preocuparle donde están alojadas las instalaciones de estos servicios. Lo único que debe preocuparle en un servicio en la nube es el método de pago (si es que lo hay) y tener un acceso a internet (Buyya, Vecchiola, & Selvi, Mastering Cloud Computing, 2013).

Los servicios en la nube se dividen en tres modelos distintos desde la perspectiva del proveedor (Zhao, Sark, & Liu, 2014):

Infraestructura como servicio

A través de una técnica llamada virtualización el proveedor es capaz de dividir, asignar y dinámicamente transformar los recursos de la nube incluyendo el proceso, el almacenamiento, las redes y otros recursos para construir sistemas virtualizados que son requeridos por el cliente. Por lo tanto el cliente es capaz de implementar y ejecutar una gran variedad de sistemas operativos y aplicaciones. Los proveedores que ofrecen este tipo de servicio son Amazon Elastic Compute Cloud (EC2) y GoGrid.

Plataforma como servicio

El proveedor ofrece una capa adicional de abstracción que es una plataforma de software en la cual se ejecuta el programa. El cliente no necesita ejecutar los recursos en la nube, pero tiene control sobre las aplicaciones ejecutadas. Tres plataformas son bien conocidas en este dominio, Google App Engine, Microsoft Windows Azure Platform y Heroku.

Software como servicio

Se provee servicios de potencial interés a una gran variedad de clientes. Los servicios son accesibles desde cualquier dispositivo a través de una delgada interfaz de usuario. Los proveedores más conocidos de estos servicios son Salesforce.com, Google Apps y Zoho.

2.1.2. Seguridad en la nube

Existen dos partes responsables de la seguridad del sistema alojado en la nube, uno es el proveedor y otro es el cliente. Sin embargo la cantidad de responsabilidad que tiene el cliente de la seguridad de sus datos depende del tipo de servicio que se esté brindando, mientras mayor sea el control que tiene el cliente en los servidores mayor es su responsabilidad (Archer, Cullinane, & Kurtz, 2011).

Como se muestra en la *Figura 2.1*, mientras menor acceso tenga el usuario, menor es su responsabilidad respecto a la seguridad. Por tanto en Software como servicio el usuario tan solo debe preocuparse por la seguridad relacionada a la interfaz, como usuario y contraseña. En cambio en Interfaz como servicio el cliente debe ocuparse de muchas cosas más.

Figura 2.1 Delineación de responsabilidades en la nube.
(Cloud Passage, 2011)

Seguridad del lado del proveedor

Ya que el proveedor es el dueño de los servidores, la seguridad que debe proveer es muy parecida a la de un centro de datos cualesquiera, por ejemplo la encriptación de los datos tanto en almacenamiento como en envío, la inclusión de firewalls o la seguridad física de los servidores. Sin embargo por la misma naturaleza de los servicios en la nube, existen algunas medidas que deben tomar los proveedores (Schulz, 2012):

- Que los datos sean encriptados tanto al transitar como al almacenarse
- La configuración y uso de Firewalls
- Medidas contra la pérdida o robo de datos.
- Revisión proactiva de la actividad en las redes, comparado a lo que se espera.
- Manejo de la encriptación de datos
- Habilitar la detección de intrusos

- Limitar adecuadamente los recursos que se brindan sin dejar de lado la productividad
- Utilizar varias capas de seguridad para los servidores, almacenamiento, redes y aplicaciones.

Seguridad del lado del cliente

La plataforma como servicio provee un ambiente de desarrollo para permitir a los desarrolladores construir aplicaciones y servicios que son alojados en la nube y accedidos por cualquier persona vía internet. El cliente en este caso tiene la responsabilidad de sus propios datos y todos los datos que genera la aplicación o servicio que está desarrollando.

Doble factor de identificación

Algunas empresas proveedoras de servicios en la nube tales como Amazon o Google tienen un mecanismo de identificación doble, llamada también identificación de dos factores (Cipriani, 2015). El primer factor es la contraseña del usuario y el segundo factor es un código de seguridad que se manda al celular del usuario para verificar en la aplicación en la nube.

Este mecanismo de identificación de dos factores se basa en la comprobación de dos factores importantes de un usuario, algo que conoce y algo que tiene. Esto es muy parecido al proceso de autenticación de un cajero automático, en el cual lo que se conoce es el pin y lo que se tiene es la tarjeta de débito. En este caso lo que conoce es la clave y lo que tiene es el dispositivo celular que posee. Esta doble capa de seguridad provee una protección adicional al cliente.

2.2. La seguridad de las contraseñas

De acuerdo a la CSA (Cloud Security Alliance), los servicios en la nube sufren principalmente de siete incidentes a su seguridad (Cloud Security Alliance, 2010), uno de estos incidentes es el robo de identidad y el otro es el robo masivo de información. Estos dos últimos ocurren el 40 por ciento de las veces de acuerdo al estudio realizado por la CSA (Cloud Security Alliance, 2013).

La pérdida o robo de información se refiere al robo de información de los usuarios pero en otros sitios o aplicaciones web. Estos sitios web no suelen tener los niveles de seguridad adecuados, e individuos maliciosos pueden aprovecharse de esto. Esta información robada de otros sitios web puede ser usada para acceder a la cuenta del usuario en sitios más seguros.

Este robo de cuenta o identidad se basa principalmente en recabar la contraseña de un usuario y luego acceder a su cuenta para ver, modificar o eliminar información privada. Los métodos de ataque a los usuarios como el phishing, el fraude o la explotación de debilidades del software aun ahora alcanzan resultados significativos (Cloud Security Alliance, 2010).

2.2.1. Mal uso de contraseñas

Otro problema que se presenta es que los usuarios no usan sus contraseñas adecuadamente. Los siguientes son problemas que tienen que ver con el mal uso que los usuarios dan a sus contraseñas.

- Según un estudio realizado por Ofcom, el comité de vigilancia en telecomunicaciones del Reino Unido, de 1805 adultos entre 16 y 25 años, se descubrió que el 55 por ciento de ellos usaba la misma contraseña para la mayoría de los sitios que visitaba (Cluley, 2013).
- Según un estudio realizado por Rainbow Technologies 64 por ciento de los usuarios finales anotaron sus contraseñas al menos una vez, comprometiendo la información empresarial (RainbowTechnology, 2003).
- El 31 por ciento de los usuarios comparte sus contraseñas con sus parejas o esposos (Larson , 2012).
- 4 por ciento de las contraseñas pueden ser adivinadas, estas son contraseñas como “password1”, 10 por ciento de las contraseñas terminan en 1, el 33 por ciento de las contraseñas tienen una longitud de 8, el 5 por ciento de las contraseñas termina con el año en el que se creo como “pitufin2016” y 4,4 por ciento de las contraseñas seguían un patrón (Fosaaen, 2015).

2.2.2. Ataques comunes de robo de identidad

Phishing

Phishing es un tipo de robo de identidad que está subiendo en popularidad entre los hackers. A través de un correo electrónico enviado a la víctima, que parece un correo de una persona o institución de confianza, pidiendo hacer una operación en un sitio web. Este sitio web es fraudulento e intenta parecerse lo más posible al legítimo, pero es manipulado por el hacker.

Una vez el usuario ingresa los datos que le pide el sitio web, el hacker tiene las credenciales del usuario (Norton, 2015).

Spear-Fishing es un tipo especial de Fishing que está dirigido a personas o empleados importantes de organizaciones o empresas (Rouse, 2011). Y para el 2015 este tipo de ataques aumentaron en un 55 por ciento respecto al 2014 (Symantec Corporation).

Pharming

Pharming es un ataque al servidor DNS de una computadora, esta computadora puede ser del cliente o un servidor DNS. El objetivo es cambiar la dirección de una IP asociada a una URL por otra URL, por ejemplo si tenemos www.misitioweb.com podemos cambiar su dirección IP para que redireccione a www.misitioweb1.com. Este segundo sitio está diseñado tal y como el original pero su objetivo es obtener las credenciales del usuario (Infosec Institute, 2015).

Cross-site Scripting

Cross-site Scripting se refiere a la inserción de código malicioso en la página web que visita el usuario, este codigo puede ser Javascript, VBScript, ActiveX, HTML, etc. Este código puede acceder a las cookies del navegador del usuario, registrar el ingreso de datos por teclado como un keylogger o mandar códigos a través de formularios de la página web que visita el usuario intentando un SQL injection (Chou, 2013). Todo esto puedo comprometer las credenciales del usuario.

SQL Injection

Es una técnica donde un usuario malicioso intenta insertar comandos SQL a través de un campo de entrada en una página web. El objetivo de este usuario es comprometer la seguridad de la aplicación web alterando comandos SQL (w3school, 2015).

Las bases de datos no relacionales también pueden sufrir de un ataque similar, este tipo de ataque es llamado NoSQL injection. En mongoDB, por ejemplo, se pueden insertar comandos especiales que tienen la misma intención de alterar o recibir informacion de la base de datos (Petko, 2014).

SQL injection es un problema que se puede tratar de varias maneras, como por ejemplo con una lista negra de palabras que no pueden ingresar a través de un campo de entrada o con parámetros especiales de SQL (w3school, 2015). Sin embargo muchos sitios poco seguros no usan este tipo

de seguridad y pueden ser vulnerados junto a datos de los mismos usuarios de otra aplicación más segura. Ya que los usuarios generalmente repiten sus contraseñas de sitio a sitio (Cluley, 2013) esta puede ser una ventaja para el hacker que intenta ingresar al sitio web seguro.

2.3. Dispositivos de hardware

En esta tesis se requiere una manera de registrar huellas digitales de manera práctica. Para ello se eligió el dispositivo Arduino como medio de comunicación y procesamiento, y el lector de huella digital 511C1R para la lectura de huellas digitales.

2.3.1. Arduino

Arduino es una plataforma de código libre basada en hardware y software de uso sencillo. El software de Arduino está diseñado para ser extendido y ejecutado en una variedad de plataformas. Puede ser usado con prácticamente cualquier componente electrónico (Aduino.cc, 2016).

Figura 2.2 Arduino Yun
(extraído de la página oficial de arduino www.arduino.org)

Existen una infinidad de modelos de Arduino, cada uno con sus propias características. Estos modelos pueden variar en tamaño capacidad y funcionalidad. Algunos modelos están diseñados exclusivamente para proyectos en robótica, otros están diseñados para funcionar con muchos dispositivos y otros para funcionar como servidores.

En esta tesis se usó el modelo Arduino Yun *(figura 2.2)*. Esta placa Arduino tiene una distribución de Linux instalada. La cual puede comunicarse con otros dispositivos a través de un módulo WiFi incluida en la placa. El Arduino Yun también lleva consigo un puerto Ethernet para conexiones alámbricas a red, usualmente usado para brindar conexión a internet al dispositivo o para conectarse a una red alámbrica (Aduino.cc, 2016).

2.3.2. Identificador de huella digital

Para lograr la identificación de huella digital se usa en este trabajo el lector de huella digital de ADH-Tech (Advanced Design House Technology). Se trata del modelo GT-511C1R *(figura 2.3)* que se caracteriza por utilizar un avanzado sensor óptico que permite tener una resolución de 450dpi (www.adh-tech.com.tw, 2016).

Figura 2.3 Lector de huella digital 511C1R
(extraido de sparkfun.com)

La mínima resolución para los lectores de huella digital utilizados en el FBI son de una resolución de 500dpi, y esta resolución es considerada estándar en la industria (Maltoni, 2003). Esto quiere decir que el lector de huella digital 511C1R es un lector estándar.

Tecnología de huella digital

La lectura de huella digital tiene 3 procesos principales (Maltoni, 2003). El primero es el registro de huellas, donde los usuarios que deben ser identificados registran sus huellas en la base de datos *(figura 2.4 A)*. Existe en este primer proceso un verificador de calidad para asegurar las futuras comparaciones de huellas digitales, este proceso suele necesitar por lo menos 3 lecturas de la huella digital del usuario para asegurar que se leyó bien la huella.

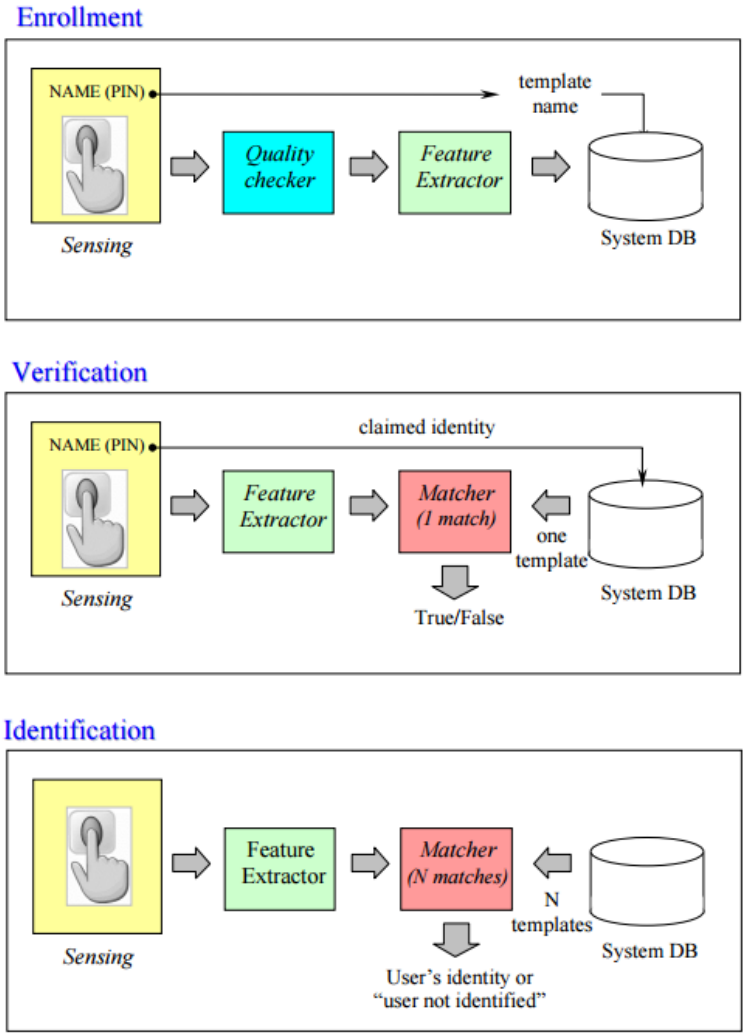

Figura 2.4 Principales procesos de la tecnología de huella digital. (Maltoni, 2003)

El segundo proceso es el de la verificación que también es llamada comparación de 1:1, en este proceso se compara la huella del usuario con una huella en la base de datos, que es la identidad que el usuario dice tener *(figura 2.4 B)*. El proceso termina con un valor booleano de respuesta que indica si el usuario es quien dice ser o no.

El tercer proceso es el de la identificación también llamada comparación 1:N, donde se compara la huella del usuario con un conjunto de las huellas registradas o también con toda la base de datos.

2.4. Seguridad

2.4.1. Seguridad de la huella digital

Seguridad Biométrica

La biométrica trata de los métodos automáticos de identificación de personas a través de uno o más rasgos conductuales o físicos intrínsecos en el ser humano. Estos rasgos son usados para dar acceso o privilegios a una persona en un sistema determinado.

En este trabajo se plantea el uso de la biometría digital para el acceso a servicios web. La biometría digital se basa en la alta variación de patrones de una huella digital para identificar únicamente a una persona. Este método es conveniente y barato, ya que todas las personas pueden usar fácil y rápidamente su huella digital. Además los dispositivos de identificación de huella digital son económicos (LiuSimon & SilvermanMark, 2011).

Falso positivo y falso negativo

El falso positivo en la identificación biométrica es la probabilidad de que una persona sea identificada correctamente siendo que esta persona no tiene la huella digital buscada. En otras palabras, la probabilidad de que se acepte una huella digital incorrecta. El falso negativo es la probabilidad de que una persona teniendo la huella digital correcta, sea rechazada por el sistema.

La Academia Nacional de Ciencias de los Estados Unidos condujo un estudio sobre la huella digital. Este estudio incluye 744 muestras de huellas digitales de 165 huellas diferentes de 21 personas. De acuerdo a este estudio el 0.1% de las veces ocurre un falso positivo al realizar pruebas con la huella digital, esto quiere decir que una vez de cada mil se detecta como positiva una huella que no debió ser. Respecto al falso negativo la probabilidad resulto ser el 0.3% de las veces. (BrandfordUlery & AustinHicklin, 2011).

2.4.2. Seguridad en la comunicación de dispositivos

La comunicación entre dispositivos requiere de varios parámetros básicos de seguridad para el envío y recepción seguro de datos.

Secure Shell

Secure Shell (SSH) es un protocolo de seguridad de redes. Cuando una computadora envía datos a otra, SSH lo encripta automáticamente y desencripta la información en la computadora receptora. SSH es una especificación de como conducir una comunicación segura sobre una red. En específico SSH cubre la autenticación, encriptación e integridad de datos sobre una red (Barrett & Silverman, 2011).

SSH es usado no solo para la comunicación de dispositivos sino también para el acceso a dispositivos para el uso de comandos remotos. En esta tesis se usa SSH para el acceso seguro al servidor y al dispositivo de huella digital.

Firewalls

Un Firewall se refiere a un dispositivo de red que bloquea ciertos tipos de comunicación en una red. Se trata de dividir la red en dos porciones, una porción segura o interna y una porción insegura o externa. El objetivo del Firewall es detener los posibles ataques a una red o un dispositivo.

En esta tesis se usara una configuración de firewall para el servidor y el dispositivo, donde solo se permite la comunicación a través de 3 protocolos que son HTTP, HTTPS y OpenSSH.

CAPÍTULO 3

MARCO APLICATIVO

3.1. Elementos aplicados

La aplicación de la identificación por huella digital en la nube en este trabajo consiste en tres elementos para realizar la correcta identificación. Estos elementos son el dispositivo de huella digital, el dispositivo cliente y el servidor.

3.1.1. Dispositivo de huella digital

El dispositivo de huella digital es el lector GT-511C1R de ADH-Tech (Advanced Design House Technology). Este dispositivo está conectado a un Arduino Yun, que viene con un módulo WiFi y una distribución Linux instalada. El Arduino tiene la finalidad de conectarse al servidor a través de Internet y mandar los datos de identificación que registra el lector de huella digital.

El dispositivo tiene como objetivo registrar nuevas huellas digitales y de identificar nuevas huellas que debe comparar con las que tiene en el registro. El usuario debe decidir si quiere identificar o registrar una huella. Para esto usa un pulsador, al presionar este pulsador se cambia de “modo registro” a “modo identificacion” o viceversa.

Ambos, el lector de huella digital y el Arduino Yun están conectados junto a elementos complementarios. Un pulsador que el usuario usa para cambiar de modo de uso. Un led naranja que indica si el pulsador anterior fue presionado correctamente. Una pantalla que indica la respuesta del servidor ante una identificación o registro. Un led verde y otro rojo que indican si

la huella digital fue leída de manera correcta o incorrecta respectivamente. Todo el circuito se muestra en la figura 3.1.

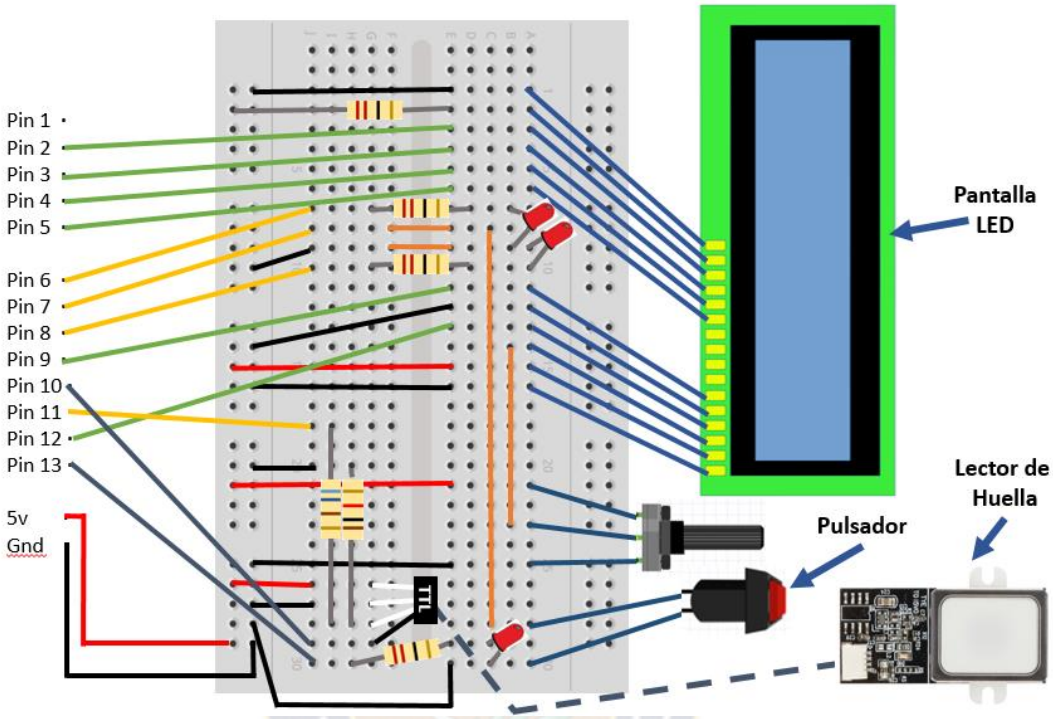

Figura 3.1 Circuito del dispositivo de huella digital

3.1.2. Servidor

El servidor tiene dos objetivos. El primer objetivo es comunicarse con el dispositivo de huella digital y registrar las acciones que se desarrollan en él, como ser registro o identificación. El segundo objetivo es ser un servidor Web, donde el usuario podrá ver las huellas registradas en su dispositivo y configurar permisos.

Para el servidor Web se utilizó MongoDB, Express y Nginx en el lado de servidor y Angular 2 para el lado cliente.

3.2. Configuración de dispositivos

3.2.1. Configuración de seguridad

La configuración de seguridad es la misma tanto en el dispositivo de huella digital como en el servidor en la nube. Ambos tienen una versión de Linux y el acceso inicial es el mismo.

El primer paso es configurar el tipo de acceso. Para ello se elimina el acceso raíz a través del usuario root. Luego se configura un nuevo usuario con acceso a través de SSH. Finalmente se

deshabilita el acceso con contraseña directa y tan solo se habilita el acceso a través de SSH. Estas tres acciones evitan el intento hacking a través de algoritmos de búsqueda completa y hacking a través del usuario root.

Luego se configura el Firewall. Dentro del servidor permitimos el acceso solamente de tres puertos, HTTP, HTTPS, OPENSSH. Esto evita el hacking a través de puertos diferentes que permiten la comunicación con nuestro servidor a intrusos y pueden revelar información relevante para el acceso al servidor.

Por último se requiere la configuración de certificado SSL, que verifica que el sitio es auténtico y confiable. Para ello se utilizó la alternativa gratuita a través del programa letsencrypt y se enlazo el sitio web para la correcta verificación del cliente. Además se utilizó una configuración de seguridad estándar que se encuentra en cipherli.st, la cual indica el tipo configuración SSL que se requiere.

3.2.2. Comunicación entre dispositivos

El servidor alojado en la nube tiene una configuración RESTful, lo cual significa que tanto el lado cliente del usuario como el dispositivo de huella digital se comunican con el servidor a través del protocolo HTTPS. Los datos que se mandan están en formato JSON.

El dispositivo de huella digital tiene un código único que lo representa y este código es validado en el lado servidor para probar la autenticidad del dispositivo. El código evita que dispositivos maliciosos intenten conectarse y realizar alguna acción como si fueran el dispositivo real.

El dispositivo y el cliente son siempre los que inician la comunicación con el servidor. El servidor se limita a responder lo que le envían (figura 3.2). El dispositivo le envía órdenes al servidor en función a la huella digital que se ingresa, y el servidor solo realiza la acción si el código enviado es el correcto y hay un mensaje de éxito respecto a la huella digital. El cliente en cambio solo pide información relacionada al estado de un proceso, como el ingreso o rechazo de una huella digital o la actualización de alguna información relevante.

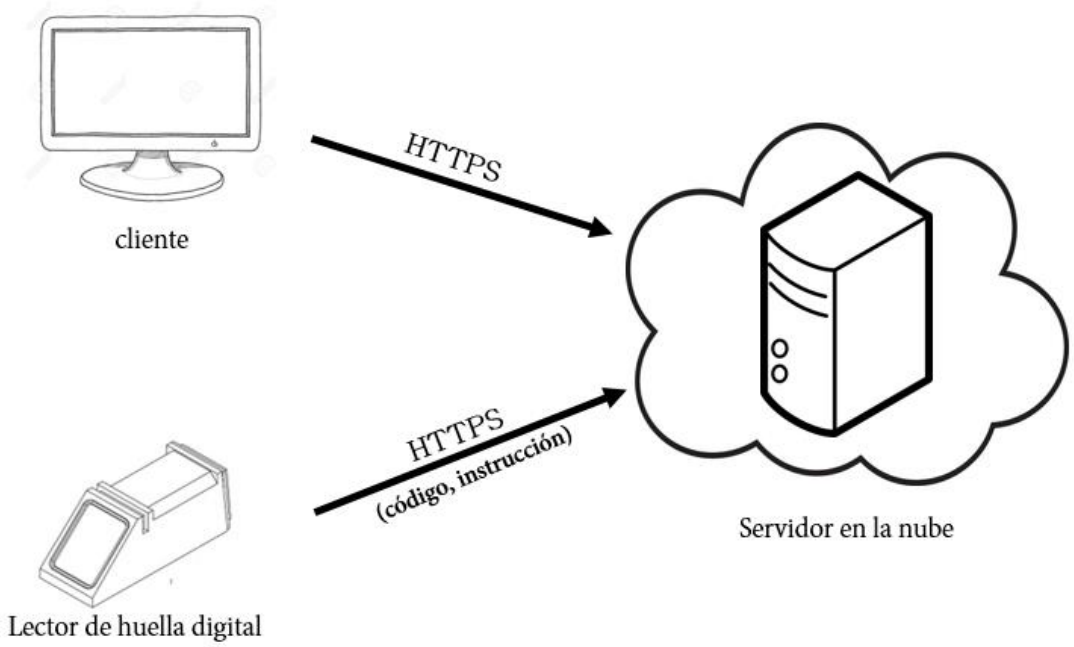

Figura 3.2 Comunicación entre el dispositivo, cliente y servidor

3.3. Funciones del dispositivo

3.3.1. Estados del dispositivo de huella digital

El dispositivo de huella digital funciona a través de un cable USB que puede ser conectado a una computadora o a un cargador de 5 Voltios. Una vez conectado muestra un mensaje exitoso y ya es utilizable.

El dispositivo tiene 2 estados principales. El primer estado es "registro" y el segundo estado es "ingreso". Estos dos estados representan las dos acciones que el dispositivo puede realizar. Es posible cambiar de estado a través del pulsador que el dispositivo tiene incorporado.

3.3.2. Registro de dispositivos

La plataforma web en la que se trabajó tiene como objetivo servir a más de un dispositivo de huella digital. Por tanto es necesario que un usuario pueda registrar su dispositivo para posteriormente usarlo en otros sitios web.

Una característica de esta plataforma web es que todo usuario que tiene una cuenta tiene un lector de huella digital, es por esto que para el registro de usuarios se pide la comprobación de un dispositivo de huella digital.

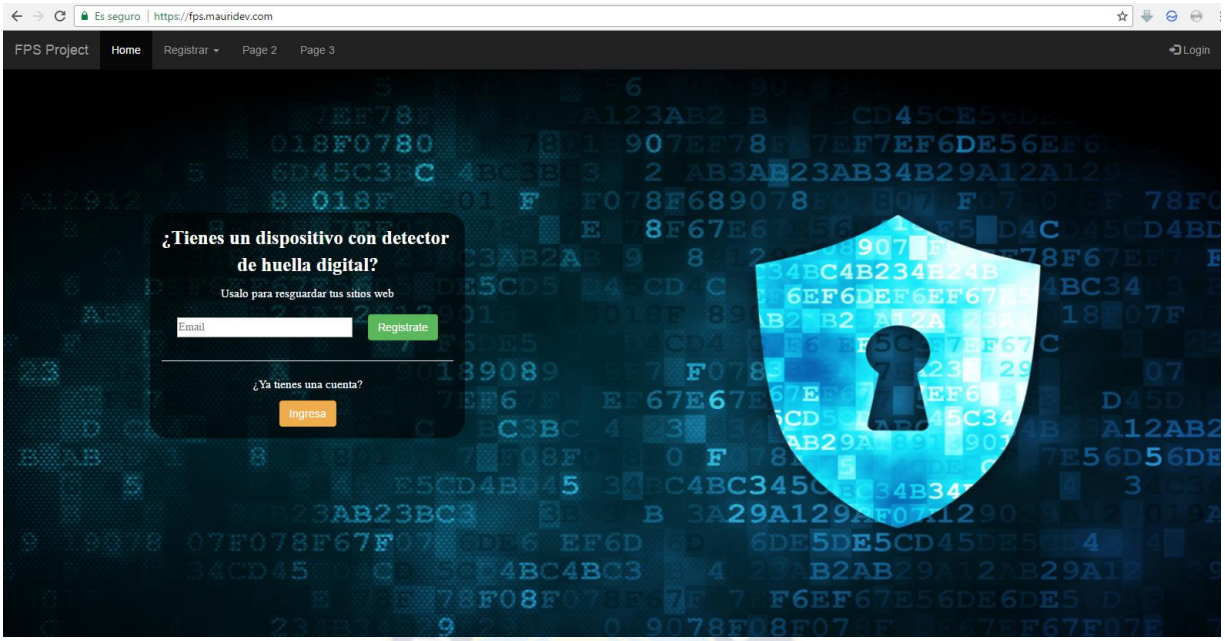

Figura 3.3 Página de Inicio para el registro de nuevos usuarios

La pantalla de inicio muestra un lugar donde ingresar un correo para registrar tu huella digital (figura 3.3). Una vez se haya ingresado el correo se pide un nombre de usuario y asignación de nombre al dispositivo para comenzar el registro (figura 3.4). Una vez ingresado los datos un mensaje de espera aparece.

Con el dispositivo conectado, se coloca en modo "registro" y se ingresa la huella digital 3 veces para registrarla correctamente. Cada vez que se pulsa el lector con la huella, una luz verde indica que se logró el registro adecuado. Si la luz es roja, se debe volver a ingresar la huella digital 3 veces.

Luego de registrar la huella 3 veces, si el registro es exitoso aparecerá un mensaje exitoso en la página web e ingresara a la nueva cuenta creada. La huella registrada es la dueña de la cuenta y con ella se ingresa al sistema posteriormente.

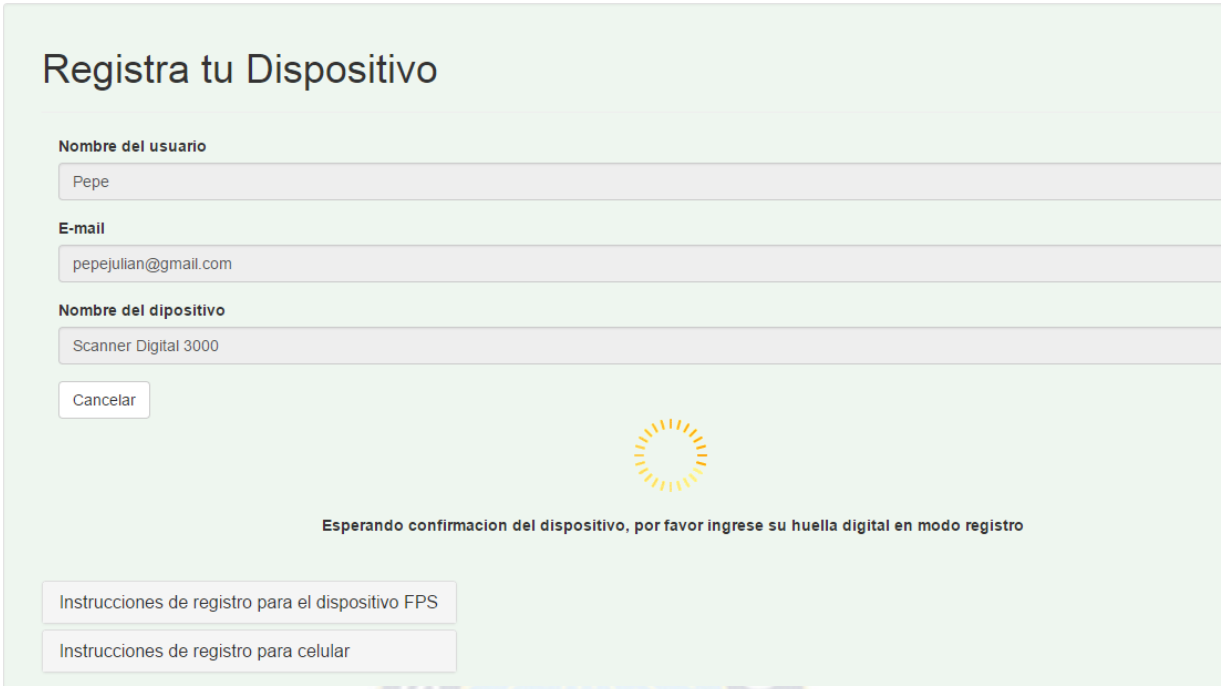

Figura 3.4 Mensaje de espera del Registro del dispositivo

3.3.3. Registro e ingreso de usuarios

Una vez el usuario tiene su cuenta activa, éste puede ingresar a su cuenta con su huella digital. En el Ingreso de usuarios de la plataforma web se pide un correo, que es el correo registrado en el registro de dispositivo. Con esto y pulsando el botón Verificar Dispositivo, la plataforma web espera una verificación de huella digital de parte del dispositivo de huella digital (figura 3.5).

Figura 3.5 Página de ingreso a la plataforma web

El dispositivo de huella digital debe encenderse y ser colocado en modo “Ingreso”, luego se coloca la huella digital y el servidor responderá con un mensaje de éxito o error, dependiendo si la huella es la que se esperaba o no.

Una vez el dispositivo y el usuario tienen su cuenta, se pueden registrar más huellas digitales en el dispositivo. Estas huellas digitales adicionales no pueden ser usadas para ingresar a la cuenta en este sitio web pero pueden habilitarse para ser usadas en otras aplicaciones web en las que se lo requiera.

Una vez en la cuenta se tiene una opción llamada “Registro de Usuarios” (figura 3.6), en ella se pide el nombre del usuario, un email de referencia y a que dispositivo se esta registrando. El proceso es muy parecido al de registro de Dispositivos ya que de la misma manera, se debe colocar el dispositivo de huella digital en modo “Registro” y registrar la huella digital 3 veces.

Figura 3.6 Registro de usuarios

Una vez completado el proceso, el nuevo usuario es guardado en la base de datos del servidor. Este usuario ahora puede usar su huella digital en los sitios donde el dueño del dispositivo indique.

CAPÍTULO 4

PRUEBAS Y RESULTADOS

4.1. Pruebas de uso

Para esta sección de pruebas de uso se toma como contraparte la identificación de dos factores que es utilizada ampliamente por varias empresas como Google o Amazon. Este doble factor de identificación incluye a la contraseña y a un código enviado al celular del usuario. El objetivo de estas pruebas es comparar los resultados del dispositivo de huella digital con los de la verificación de código.

En esta prueba se quiere ver si el método por dispositivo de huella digital planteado en esta tesis tiene un tiempo de uso estadísticamente menor, mayor o igual al de su contraparte, el de confirmación por código a celular. Se recogerán dos muestras, una para cada método. La muestra número uno representa al dispositivo de huella digital y la muestra numero dos a la confirmación vía celular.

Muestra #1

Para la muestra número uno se recolectara información del tiempo de uso de 15 personas. Cada persona registrara su huella digital en el servidor y luego se le presentara una pantalla para realizar una acción, siendo en este caso la eliminación de un usuario. Una vez el usuario oprima

el botón de eliminación, el cronometro comienza a correr. El usuario hace la verificación de la huella digital y realiza la eliminación. El cronometro se detiene cuando el usuario recibe un mensaje de éxito del servidor.

	Tiempo Huella Digital (seg)	Verificacion doble de google (seg)
Persona #1	15,1	22
Persona #2	17,2	32,9
Persona #3	12,9	22,5
Persona #4	18,7	37,3
Persona #5	13,5	41,6
Persona #6	16,6	32,7
Persona #7	21,8	37,6
Persona #8	15,7	34,4
Persona #9	16,8	38,1
Persona #10	14,8	27,4
Persona #11	19,2	28,7
Persona #12	15,6	28,2
Persona #13	15,8	26,7
Persona #14	16,4	31,1
Persona #15	14,7	30,6
Promedio	16,32	31,45
Desviacion Standard	2,195	5,532
Varianza	4,822	30,6

Tabla 4.1 Resultado de las muestras extraídas

Muestra #2

Para la muestra número dos se hace la recolección de información de las mismas 15 personas de la muestra número uno. Sin embargo en esta muestra se utiliza el servicio de doble factor de Google, que es un servicio de confirmación de código vía celular. El usuario debe oprimir el botón de envió de código de Google, tras lo cual el cronometro comienza a correr. Una vez el usuario reciba el código en su celular, lo confirme en el sitio web y se le muestre el mensaje de éxito de Google, el cronometro se detendrá.

El resultado de ambas muestras se muestra en la tabla 4.1.

Procedimiento

$$Hipotesis\ nula\ H_0: las\ muestras\ son\ estadisticamente\ iguales$$

$$Hipotesis\ alternativa\ H_1: las\ muestras\ son\ estadisticamente\ diferentes$$

Nuestra hipótesis nula indica que el tiempo necesario de identificación de una persona con el dispositivo de huella digital es estadísticamente igual al que tarda en utilizar el doble factor de identificación de Google. La hipótesis alternativa indica que existe una diferencia estadísticamente significativa entre estos tiempos. Por ser las muestras pequeñas se utilizará t de Student. Se trabajará con un alfa de 0,05 y 28 grados de libertad.

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 \neq \mu_2$$

Se calcula la varianza conjunta de ambas muestras.

$$S^2 = \frac{(n_1 - 1)S_1^2 + (n_2 - 1)S_2^2}{n_1 + n_2 - 2} = 89{,}077$$

Con lo cual se puede calcular el valor aproximado de la distribución t.

$$t = \frac{\overline{X_1} - \overline{X_2}}{S\sqrt{\frac{1}{n_1} + \frac{1}{n_2}}} = 4{,}6$$

Comentarios

Según la tabla de la distribución t, para $\alpha = 0{,}05$ de doble cola el valor de t es 2,048. Dado que el valor de t hallado anteriormente es mayor al valor de la tabla se puede concluir que el tiempo que tarda un usuario en utilizar el servicio de huella digital es diferente al que tarda en usar el servicio de doble identificación de Google. Más específicamente el uso de la huella digital es estadísticamente menor que el de su contraparte.

4.2. Pruebas de seguridad

La seguridad del dispositivo de huella digital se basa principalmente en que el usuario no necesita memorizar una contraseña y tan solo necesita su huella digital para acceder a sus

servicios web. Sin embargo, existen algunas otras consideraciones de seguridad que tomar en cuenta en especial considerando la seguridad del dispositivo como tal y de la aplicación web.

4.2.1. Parámetros de seguridad de la OWASP

Siendo que el dispositivo de huella digital usado en este trabajo es un dispositivo del Internet de las cosas, se utilizara la guía de pruebas de seguridad de dispositivos del Internet de las cosas de OWASP. El cual consiste en once parámetros básicos de seguridad que deben cumplir los dispositivos del internet de las cosas.

OWASP es una organización dedicada a la seguridad de la información, su sigla traducida al español significa "Proyecto de seguridad de aplicaciones libres en la Web". De los once parámetros para verificar que un dispositivo del internet de las cosas es seguro, seis aplican al trabajo presentado.

Categoria	Consideracion de seguridad	Dispositivo	Servidor	Aplicación Web
Interfaces Web inseguras	Determinar si se permiten contraseñas debiles			
	Determinar el uso de HTTPS para la proteccion de la informacion			
	Determinar la posibilidad de cambio de contraseña			
	Determinar si se verifican los datos contra vulnerabilidades como la injeccion SQL			
	Determinar si las aplicaciones web utilizan algun tipo de firewall			
	Determinar si existe un mecanismo de bloqueo de cuentas			
Autorizacion Insuficiente	Uso de contraseñas fuertes donde es necesaria la autenticacion			
	Determinar la separacion de roles			
	Implementacion de seguridad de dos factores donde sea posible			
	Permitir el cambio de usuario y contraseña			
Servicios de Red inseguros	Determinar si la solucion puede lidiar con ataques DoS			
	Asegurar que la solucion no tenga puertos de prueba que puedan comprometer la seguridad			
Falta de Encriptacion	Determinar el uso de comunicación encriptada entre dispositivos y entre dispositivos e Internet			
	Determinar si se usan practicas standares de encriptacion			
	Determinar que la solucion no usa protocolos privados de encriptacion			
	Determinar que el firewall esta siempre activo			
Seguridad fisica insuficiente	Determinar si el dispositivo utiliza la menor cantidad de puertos			
	Determinar si el dispositivo puede ser accedido por metodos diferentes			
Software/Firmware	Determinar si el dispositivo recibe actualizaciones constantes			

Tabla 4.2 Requisitos de seguridad de la OWASP

En la tabla 4.2 se puede observar las seis categorías que tomamos en cuenta para probar la seguridad. Se puede ver que no todas las consideraciones aplican a los tres, dispositivo, aplicación web o servidor, ya que son diferentes.

Para el dispositivo de huella digital aplican trece consideraciones de seguridad, de las cuales se cumplen las trece. Para el servidor aplican once y de ellas diez se cumplen. Para la aplicación Web se cumplen doce de trece. El factor que falta en la elaboración de trabajo es la consideración de ataques DoS, el cual no tiene que ver con la identificación de usuarios.

4.2.2. Test de seguridad a la aplicación Web

SSL Labs es un sitio que te permite hacer pruebas de seguridad de sitios web. El test prueba cuatro parámetros, la seguridad del certificado Web, el soporte de protocolo, el intercambio de clave y la seguridad del cifrado.

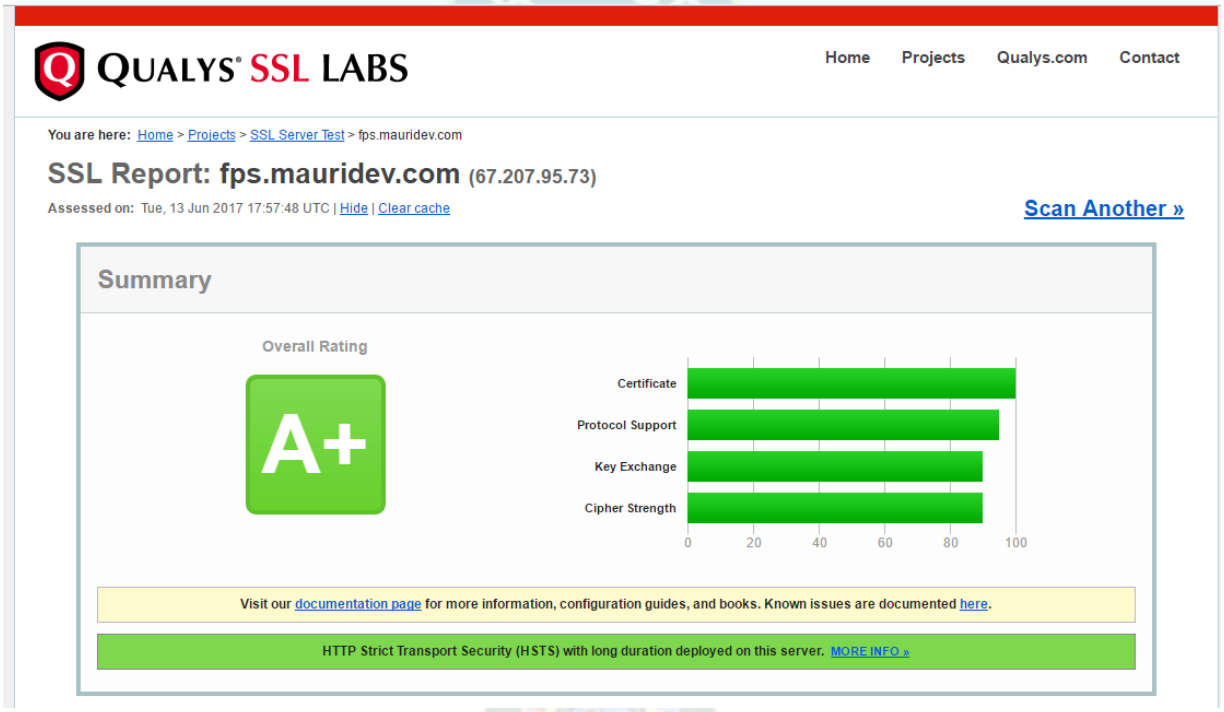

Figura 4.1 Resultado del test de seguridad SSL

El sitio web que se tiene alojado tiene un nivel de seguridad A+, según el test de seguridad de SSL Labs.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Al haber construido un dispositivo de huella digital que trabaje con un servidor en la nube se logró la identificación única de usuario y su registro al sistema por medio de la huella digital. Aun así, no solo se trata de la identificación única de usuario, sino del servicio que se ofrece en la nube para dispositivos de huella digital, donde cualquier usuario con uno de estos dispositivos se registra o identifica por medio del servicio en la nube o utiliza el servicio API RESTful para usar la identificación biométrica en sitios web o aplicaciones de su preferencia.

A través de una muestra tomada de 15 personas se comparó el servicio de identificación de huella digital propuesta en este trabajo y la verificación vía celular de Google. Se encontró que la verificación vía celular de Google toma estadísticamente más tiempo que la identificación de huella digital.

Luego de probar la seguridad del servidor Web con una prueba por Internet de seguridad SSL, se consiguió una calificación A+. Esto significa que el servidor cumple con los requisitos más indispensables de seguridad y con las certificaciones correspondientes. Posteriormente se utilizó la lista de requerimientos de seguridad de OWASP para dispositivos en el Internet de las cosas.

Se encontró que el dispositivo de huella digital, el servidor y el cliente cumplen con los requerimientos de seguridad al menos al 90 por ciento.

5.2. Recomendaciones

El dispositivo de huella digital usado tiene un almacenamiento interno de 120 huellas digitales. Sin embargo el Arduino Yun cuenta con una ranura SD para almacenamiento extra. En caso de necesitar más de 120 huellas digitales se recomienda configurar el dispositivo de huella digital para usar la ranura SD.

El servicio API RESTful puede trabajar con cualquier dispositivo de huella digital siempre y cuando el dispositivo sea configurado para trabajar con el servicio API. Se recomienda que se utilicen dispositivos móviles con identificador de huella digital para que el servicio tenga un mayor alcance.

BIBLIOGRAFIA

Aduino.cc. (2016). *arduino.cc*. Obtenido de www.arduino.cc

Archer, J., Cullinane, D., & Kurtz, P. (2011). *Cloud Security Alliance.* Obtenido de https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

Avgerou, C. (2007). *ICT and citizens trust in government: lessons from electronic voting in Brazil.* Obtenido de http://www.ifipwg94.org.br/fullpapers/R0098-1.pdf

Barrat, J., Goldsmith, B., & Turner, J. (2012). *International Experience with E-Voting.* Obtenido de http://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf

Barrett, D., & Silverman, R. (2011). *The Secure Shell.* O'reilly.

Brandford, U., & Austin, H. (2011). *National Academy of Sciences US.* Obtenido de http://www.pnas.org/content/108/19/7733.full.pdf

Buyya, R., Vecchiola, C., & Selvi, T. (2013). *Mastering Cloud Computing.* Morgan Kaufmann.

Buyya, R., Vecchiola, C., & Selvi, T. (2015). *Mastering Cloud Computing Foundations and Applications Programming.* Morgan Kauffman.

Chou, T.-S. (2013). *Security Threats on Cloud Computing.* Obtenido de http://airccse.org/journal/jcsit/5313ijcsit06.pdf

Cipriani, J. (15 de Junio de 2015). *CNET.* Obtenido de www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

Cloud Passage. (2011). *Cloud Passage*. Obtenido de https://blog.cloudpassage.com/2011/06/06/whos-responsible-for-security-in-a-cloud/

Cloud Security Alliance. (2010). *Cloud Security Alliance.* Obtenido de https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance. (2013). Cloud Computing Vulnerabiity Incidents; A statistical Overview. Obtenido de https://www.cert.uy/wps/wcm/connect/certuy/abfd80ca-3142-4d28-b99c-e8f841568dde/Cloud_Computing_Vulnerability_Incidents.pdf?MOD=AJPERES

Cluley, G. (23 de Abril de 2013). *Most net users use the same passwords for most websites*. Obtenido de Naked Security: https://nakedsecurity.sophos.com/2013/04/23/users-same-password-most-websites/

Dzieduszycka, S., & Murray, J. (2015). *The Future of Voting.* Obtenido de https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf

Everett, S. P. (mayo de 2007). *google schollar.* Obtenido de http://chil.rice.edu/alumni/petersos/EverettDissertation.pdf

Ford, N. (2012). *Essential Guide to Using the Web for Research.* Sage.

Fosaaen, K. (2015). *Netspi*. Obtenido de https://blog.netspi.com/netspis-top-cracked-passwords-for-2014/

Genes, R. (2011). *Transition to the cloud, The case for a code of practice.* Cloud Industry Forum.

Gertz, A. (2015). *The Breach Level Index*. Obtenido de http://blog.gemalto.com/security/2016/03/03/2015-data-breaches-by-the-numbers/

Granger, S. (2001). *Fundamentos de la Ingeniria Social.* Obtenido de http://www.123seminarsonly.com/Seminar-Reports/021/19676093-Social-Engineering-Fundamentals.doc

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, P. (1997). *Metodologia de la Investigacion.* MC Graw Hill.

Infosec Institute. (2015). *Infosec*. Obtenido de http://resources.infosecinstitute.com/pharming-attack/

Jones, D., & Simons, B. (2012). *Broken Ballots.*

Larson , T. (2012). *Password Survey on Norway.* Obtenido de http://passwords12.at.ifi.uio.no/NorSIS_Passwords12.pdf

Leyden, J. (23 de Diciembre de 2014). *JP Morgan mega hack was a simple two factor auth fail*. Obtenido de The Register: http://www.theregister.co.uk/2014/12/23/jpmorgan_breach_probe_latest/

Liu, S., & Silverman, M. (2011). A practical Guide to Biometric Security Technology. Obtenido de https://intranet.dcc.ufba.br/pastas/gaudi/biometrica/papers/id/PraticalGuideBiometric-00899930.pdf

Maio, D., Jain, A., Prabhackar, S., & Maltoni, D. (2009). *Hanbook of Fingerprint Recognition.* Springer. Obtenido de https://books.google.com.bo/books?hl=en&lr=&id=1Wpx25D8qOwC&oi=fnd&pg=PR11&dq=optical+fingerprint+algorithms&ots=9xRZ4Ujtc4&sig=TSNHOwZ5O6x6Lm_l0N9hQOzTm5E#v=onepage&q=hase&f=false

Maltoni, D. (2003). *Authentication and Recognition.* Obtenido de http://pbi.gov.bd/images/article/fingerprint.pdf

MURRAY, J. (10 de Julio de 2010). *google schollar.* Obtenido de https://www.usvotefoundation.org/sites/default/files/E2EVIV_usability_report.pdf

Norton. (2015). *Norton by Simantec*. Obtenido de http://us.norton.com/7-tips-to-protect-against-phishing/article

Petko, D. (2014). *Blog Securify*. Obtenido de http://blog.websecurify.com/2014/08/hacking-nodejs-and-mongodb.html

Quick, M., Hollowood, E., Miles, C., & Hampson, D. (6 de Mayo de 2016). *Information is Beautiful*. Obtenido de http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

RainbowTechnology. (2003). *Reinbow Technology*. Obtenido de http://www.m2.com/m2/web/story.php/200323D9D4562554D6BD85256D18002B280D

Rouse, M. (2011). *Search Security*. Obtenido de http://searchsecurity.techtarget.com/definition/spear-phishing

Schulz, G. (2012). *Cloud and Virtual Data Storage.* CRC Press.

Scrum Alliance. (2016). *Scrum Alliance*. Obtenido de https://www.scrumalliance.org

Sherman, A. T. (2010). *ACM Digital Library.* Obtenido de http://dl.acm.org/citation.cfm?id=2049323

Siani, P., & George , L. (2011). *Privacy and Security for cloud computing.* Springer.

Silveira, V. (2012). *Linkedin*. Obtenido de https://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised

Symantec Corporation. (s.f.). *Symantec.* Obtenido de https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf

Vallabhu, H. (2012). *Biometric Authentication as a Service.* Obtenido de international Journal of Soft Computing.

Venezia, P. (23 de Junio de 2014). *Murder in the Amazon Cloud*. Obtenido de Info World: http://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html

w3school. (2015). *w3school*. Obtenido de http://www.w3schools.com/sql/sql_injection.asp

Walters, R. (26 de Marzo de 2016). *Insecure Password or Insecure People?* Obtenido de Cloud Industry Forum: http://www.cloudindustryforum.org/content/insecure-passwords-or-insecure-people

Wolf, P. (2011). *Introducing Electronic Voting.* Suecia: Bulls Graphics. Obtenido de http://www.eods.eu/library/IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf

www.adh-tech.com.tw. (2016). *ADH-Tech*. Obtenido de http://www.adh-tech.com.tw/

Xihua. (14 de Noviembre de 2015). Bolivia encara 10 elecciones en una década a un costo de US$140 millones. *America Economia*. Obtenido de http://www.americaeconomia.com/politica-sociedad/politica/bolivia-encara-10-elecciones-en-una-decada-un-costo-de-us140-millones

Zhao, L., Sark, S., & Liu, A. (2014). *Cloud Data Management.* Springer.

ANEXOS

Anexo A – Metodología IOT

Esta metodología está diseñada especialmente para el desarrollo de soluciones del Internet de las cosas. Consta de un conjunto de pasos iterativos para llegar a la solución final.

- **Co-crear:** Comunicación con los usuarios finales para identificar problemas o puntos de conflicto de manera no técnica.
- **Idear:** Simplificar la discusión para comunicar los requerimientos de forma técnica a los diseñadores y desarrolladores.
- **Q&A:** Convertir los conceptos discutidos en requerimientos, para analizar la solución y buscar opciones.
- **IOT OSI:** Mapear los requerimientos para validar la arquitectura e infraestructura a utilizarse.
- **Prototipo:** Construcción de prototipos que iteran hacia un producto mínimo viable.
- **Implementación:** La implementación continua ayuda a cerrar el ciclo de retroalimentación y mejora la colaboración.