Sistema de almacenamiento en la nube utilizando reconocimiento facial para el cifrado de la información

Trabajo Terminal No. 2020-A068

Alumno: García Sánchez Alexis Andrés

Directores: M. en C. Marco Antonio Dorantes González

alexis.gs.0912@gmail.com

Resumen – El presente trabajo tiene el propósito de desarrollar un sistema de almacenamiento en el cual la información sea cifrada por medio de criptografía asimétrica la cual utiliza dos llaves, una pública y una privada, las cuales serán generadas utilizando reconocimiento facial. Mediante el uso de criptografía asimétrica se reduce el riesgo de que un atacante tenga acceso a la información ya que la llave privada se generará a partir de la información biométrica del usuario lo cual impedirá que la llave caiga en manos de un actor malicioso. Así se busca ofrecer una alternativa para proteger la información que se almacene en el sistema de posibles amenazas y vulnerabilidades que pueden afectar su confidencialidad, integridad y disponibilidad.

Palabras clave – cómputo en la nube, biométricos, criptografía.

1.Introducción

En los últimos años, el almacenamiento en la nube se ha vuelto una de las principales herramientas tanto para uso público como privado y recientemente una de las necesidades más grandes es la protección de los datos que se almacenan en la nube, información sensible a criterio del usuario, para lo cual se emplean diferentes métodos de cifrado. Si bien la necesidad principal que se busca cubrir con estos métodos es proteger la información, en ocasiones la seguridad de las llaves tanto públicas como privadas también se ve comprometida.

- Cifrado de clave privada: este tipo de cifrado, también conocido como simétrico, utiliza solo una clave que tanto el emisor como el receptor deben poseer. El emisor utiliza la clave para cifrar el mensaje y el receptor descifra el mensaje con la misma clave. La clave no debe compartirse con nadie más que con el emisor y el receptor para garantizar la transmisión segura del mensaje. [1]
- Cifrado de clave pública: en este tipo de cifrado, también llamado asimétrico, cada usuario debe tener dos claves, una pública y una privada, el emisor cifra el mensaje con su clave privada y el receptor lo descifra con la clave pública del emisor, las claves públicas de ambos serán compartidas mientras que la clave privada debe estar en posesión únicamente de su respectivo usuario. [1]

Aunque en criptografía de clave pública, la clave privada es conocida únicamente por su respectivo usuario, siempre existirá el riesgo, por mínimo que parezca, de que dicha llave caiga en manos de personas no autorizadas, por lo que con el presente trabajo, se busca implementar un algoritmo de generación de llaves por medio de reconocimiento facial, con lo cual la llave privada se encontrará en la biometría facial del usuario, aumentando así la confidencialidad de la llave.

Existe una gran variedad de servicios y aplicaciones que ofrecen almacenamiento de archivos en la nube y métodos para la protección de los mismos así como reconocimiento de biometría facial, considerando las particularidades del presente proyecto, en la Tabla 1 se muestra una comparación de servicios con características similares, algunos enfocados en almacenamiento y cifrado de archivos, y otros enfocados al reconocimiento facial.

Estado del arte

SOFTWARE	CARACTERÍSTICAS
AceroDocs	Es una aplicación que ofrece la protección de documentos mediante cifrado, que incluye una función de protección remota, conocida como IRM (Information Rights Management) [2], para documentos en cualquier formato, que el usuario considere sensibles, una vez cifrados, los documentos se pueden compartir en la nube. [2,3]
MEGA	En un servicio de almacenamiento en la nube que ofrece un cifrado punto a punto de todos los datos transferidos y almacenados. También cifra la contraseña de acceso para garantizar a los usuarios que ni el propio servicio tendrá acceso a la información almacenada en él. [4]
Sistema Generador y Modelador de Retratos Hablados K-Rax 3D	Trabajo Terminal desarrollado en la ESCOM, el proyecto es un sistema capaz de generar y modelar retratos hablados en tercera dimensión y simular su progresión en edad. El sistema facilitará la identificación de delincuentes y personas extraviadas.[5]
Face ID Lock Screen	Es una aplicación de identificación de rostros que sirve para configurar el desbloqueo del smartphone utilizando biometría facial. Para ello, al instalar la aplicación el primer paso es registrar un rostro, de modo que el software va a leer detalladamente todos los rasgos característicos del usuario. Una vez hecho, cada vez que se desee desbloquear el dispositivo, el sistema solo lo permitirá si hay un 100% de coincidencia en la identificación. [6]
Vault	Es una herramienta diseñada con el objetivo de bloquear el acceso a las apps móviles, ocultar material audiovisual como fotos o videos y hacer un backup en la nube personal de cada usuario. Uno de los elementos (opcionales) de seguridad que ofrece a los usuarios es el desbloqueo mediante reconocimiento facial.[6]
AppLock Face	Esta aplicación de seguridad de datos hace énfasis en el desbloqueo mediante el reconocimiento de voz y rostro del usuario. Además, permite bloquear el acceso a mensajerías instantáneas, redes sociales, información bancaria y galería de fotos y video. Tiene dos niveles de seguridad: voz o rostro, o voz y rostro. El primero es opcional, y el usuario puede escoger si desbloquea su móvil mediante una frase o sólo con mostrar su rostro. El segundo nivel de seguridad es el más avanzado y combina ambos elementos para garantizar de que solo el usuario pueda acceder al dispositivo. [6]
Railer	Es una app para control de accesos y gestión de horarios para personal. Provee un servicio que por medio del reconocimiento biométrico, registra horas de entrada y salida de personal. También provee un análisis con gráficas cronológicas de asistencias y ausencias. Está dirigida para pequeñas y medianas empresas y escuelas y significa un avance en el ámbito laboral, ya que ha disminuido el absentismo o la impuntualidad. [6]

Luxand Face Recognition	Esta aplicación se limita a sólo al reconocimiento facial de los usuarios, sin ninguna otra cualidad o función, pero tiene una alta eficacia gracias a que hace uso de un motor biométrico avanzado que sirve como recurso para desarrolladores que quieran construir con base en esta tecnología. [6]
Boxcryptor	Boxcryptor es una aplicación que cifra archivos y carpetas en servicios de almacenamiento en la nube. Cada usuario cuenta con un par de claves RSA de 4096 bits de longitud, así como claves AES para cifrar y descifrar archivos. [7]

Tabla 1. Resumen de productos similares

2.Objetivo

Desarrollar un sistema de almacenamiento en la nube que emplee reconocimiento facial para la generación de las llaves de cifrado de la información que se almacene en la nube.

Objetivos específicos:

- Implementar un algoritmo generador de llaves de cifrado por medio de reconocimiento facial para fortalecer la seguridad de la información almacenada en la nube.
- Desarrollar un módulo de cifrado en el cual se hará uso de las llaves generadas por reconocimiento facial
- Desarrollar un módulo para gestionar las diferentes funcionalidades del sistema y el intercambio de información dentro del mismo.
- Desarrollar un módulo para el control de la información personal del usuario, buscando garantizar la confidencialidad de los datos.

3.Justificación

Actualmente, la mayoría de los usuarios utilizan servicios de almacenamiento en la nube, por lo que es importante mantener su información segura, sin embargo, estos servicios están expuestos a vulnerabilidades importantes [8], por lo que es recomendable considerar mejoras en la estructura de este tipo de sistemas y nuevas implementaciones de seguridad. Aunado a esto, el reconocimiento facial es una tecnología que ha crecido y ha tenido muchas aplicaciones, no obstante, es limitada la información para el uso de las tecnologías biométricas para la generación de llaves, por lo cual implementarla en un sistema de estas características representa una alternativa en el manejo seguro de la información y llaves de cifrado así como en la aplicación de esta tecnología..

Las vulnerabilidades no pueden evitarse, pero es posible disminuir el riesgo, algunos problemas que se buscan mitigar son:

Pérdida de datos: se considera pérdida de datos el caso en que un usuario pierde u olvida las claves con las que cifró su información antes de subirla a la nube, ya que posteriormente, no podrá descifrar ni recuperar sus datos, la idea de implementar el reconocimiento facial es que para generarlas, como ya se mencionó previamente, se partirá de la información biométrica del usuario, así el individuo portará su llave en todo momento.[9]
Confidencialidad: se busca que únicamente el usuario o usuarios autorizados puedan acceder a la información almacenada en el sistema con el correspondiente cifrado.
Además, el sistema sería una alternativa de software libre a otros productos similares, buscaría cubrir la necesidad de las empresas y los usuarios de disponer información confidencial en la nube para agilizar sus procesos de trabajo y en el desarrollo se reflejarán los conocimientos y habilidades adquiridas a lo largo de la carrera, en especial de asignaturas como Criptografía, una unidad de aprendizaje esencial para un proyecto de esta naturaleza.

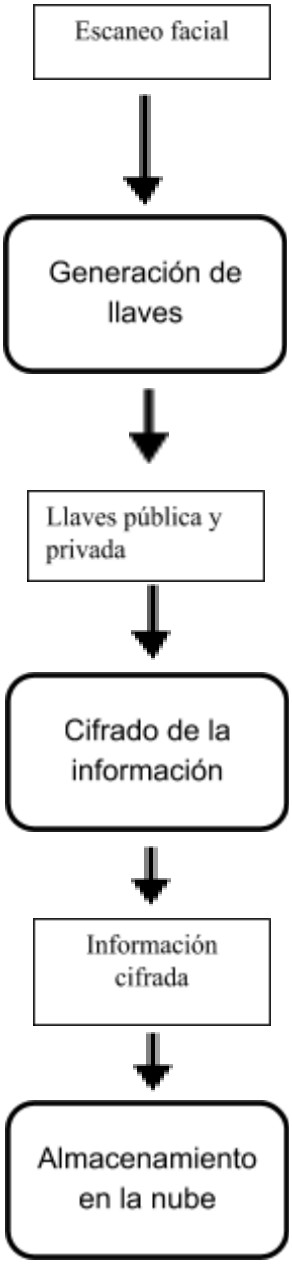
Por otra parte, en México, muchos usuarios tienen una deficiente cultura en seguridad de la información, por lo que el presentar aplicaciones y proyectos que ofrezcan estos servicios podría acercar a los usuarios a reflexionar sobre la atención que ponen a la seguridad de sus datos ya que.

4.Productos o Resultados esperados

Para la evaluación de TT1 se espera contar con los prototipos de: el sistema de almacenamiento en la nube con el módulo de gestión y control de datos y el prototipo del módulo de cifrado para la generación de las llaves además de la documentación correspondiente al manual de usuario y manual técnico.

Para TT2 los prototipos esperados son el sistema completo con el módulo de cifrado completamente integrado y funcional, así como el reporte final y los manuales técnico y de usuario.

Arquitectura del sistema:



5.Metodología

Modelo basado en prototipos:
También conocido como modelo de desarrollo evolutivo, se inicia con la definición de los objetivos globales para el software, luego se identifican los requisitos conocidos y las áreas del esquema en donde es necesaria más definición. Este modelo se utiliza para dar al usuario una vista preliminar de una parte del software. Este modelo es básicamente prueba y error ya que si el usuario no está conforme con una parte del prototipo significa que la prueba falló y se deben hacer las correcciones pertinentes hasta que el usuario quede satisfecho. Además, el prototipo debe ser construido en poco tiempo, usando las herramientas adecuadas y sin una gran inversión, pues a partir de que este sea aprobado, se puede iniciar el verdadero desarrollo del software. Al construir el prototipo nos aseguramos de que nuestro software será de mejor calidad y que su interfaz sea amigable para el usuario.

Etapas

- Recolección y refinamiento de requisitos
- Modelado, diseño rápido
- Construcción del Prototipo
- Desarrollo, evaluación del prototipo por el cliente
- Refinamiento del prototipo
- Producto de Ingeniería

Ventajas

- No modifica el flujo del ciclo de vida
- Reduce el riesgo de construir productos que no satisfagan las necesidades
- Reduce costo y aumenta la probabilidad de éxito
- Exige disponer de las herramientas adecuadas
- Este modelo es útil cuando se conocen los objetivos generales para el software, pero no identifica los requisitos detallados de entrada, procesamiento o salida.
- También ofrece un mejor enfoque cuando el responsable del desarrollo del software está inseguro de la eficacia de un algoritmo, de la adaptabilidad de un sistema operativo o de la forma que debería tomar la interacción humano-máquina.

Los prototipos considerados para el desarrollo y la implementación son:

TT1:

1. Prototipo 1: el sistema de almacenamiento en la nube, con los módulos de gestión y control de datos
2. Prototipo 2: módulo de reconocimiento facial

TT2:

1. Prototipo 3: módulo de cifrado
2. Prototipo 4: integración del sistema de almacenamiento con el módulo de cifrado y de reconocimiento facial.

6.Cronograma

Actividad	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Análisis y diseño del sistema										
Prototipo 1: Sistema de almacenamiento, análisis y desarrollo del backend										
Prototipo 1: Sistema de almacenamiento, análisis y desarrollo del frontend										
Prototipo 2: análisis e implementación del componente empleado en el módulo de reconocimiento facial										
Documentación y pruebas										
Evaluación de TTI										
Prototipo 3: análisis, desarrollo e implementación del módulo de cifrado										
Prototipo 4: integración de todos los módulos que componen el sistema										
Pruebas del sistema integrado										
Reingeniería										
Documentación del producto final.										
Evaluación de TTII.										

7.Referencias

[1] IBM. (2014, Abril 25). “Criptografía de clave pública”, [Internet], Disponible en https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm

[2] A. Martinez (2014, Febrero 24), “Information Rights Management”, [Online], Disponible en https://www.incibe-cert.es/blog/information-rights-management

[3]AceroDocs (2016) [Internet] Disponible en https://www.acerodocs.com/es/

[4]MEGA [Internet] Disponible en https://mega.nz

[5] A. Ambrosio, J.M. Cruz Flores, M.A. Rojas Mejía, J.A. Santiago Jaime, “Sistema Generador y Modelador de Retratos Hablados K-Rax 3D”, Trabajo Terminal, IPN-ESCOM, Ciudad de México, México, 2007.

[6] C. Crespo (2019, Septiembre 17). “Las Mejores Aplicaciones con Reconocimiento Facial: TOP 2020, [Internet], Disponible en https://tuapppara.com/reconocimiento-facial/

[7] Boxcryptor (2011) [Internet] Disponible en: https://www.boxcryptor.com/es/technical-overview/

[8] Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights report. Cloud Security Alliance, 2017.

[9] Rodríguez, Juan, Algoritmo de generación de llaves de cifrado basado en biometría facial. Revista Inventum. Nº 19 pp. 43 - 53, Julio-Diciembre 2015.

8.Alumnos y directores

Alexis Andrés García Sánchez - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, especialidad Sistemas, Boleta: 2016630141, Tel. 5521852731, email: alexis.gs.0912@gmail.com

Firma: _____

Marco Antonio Dorantes González. - Maestro en Ciencias de la Computación, CINVESTAV, Ing. En Electrónica, ITO, Profesor de la ESCOM desde 1996, Sus áreas de interés son: Cómputo Móvil, Ingeniería de software, Base de Datos, ha sido director de más de 80 trabajos terminales a la fecha, revisor técnico de libros de las áreas de interés para diferentes editoriales (McGraw Gill, Thompson, Pearson Education, entre otros), ha participado en diversos proyectos de investigación y ha ocupado diversos cargos administrativos en el IPN, también cuenta con experiencia en el sector industrial en el área de instrumentación y electrónica; ha realizado estudios de diplomado en diversas áreas, ha participado en diversos programas de televisión y publicaciones en revistas de carácter científico, Tel.: 57296000 Ext. 52032 correo-e: mdorantesg@ipn.mx

Firma: _____