Sistema para la sincronización y gestión segura de archivos críticos en las organizaciones

Mario Andrés Hurtado Sáenz, Daniel Andrés Donado Avendaño
Maestría en Seguridad de la Información. Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes.
Bogotá, Colombia. Noviembre 2024

***Resumen*— Este artículo analiza las problemáticas que se pueden presentar en ciertos contextos al no tener una herramienta eficaz para la gestión de archivos, que permita garantizar su disponibilidad. También propone un sistema para la sincronización y gestión segura de estos. Se muestra como esta aplicación puede proporcionar la integridad, autenticidad y disponibilidad de los archivos, al igual que proporcionar una mayor conveniencia para los usuarios, utilizando métodos de autenticación *passwordless* y ofreciendo una búsqueda sobre los archivos cifrados, por medio de palabras clave.**

Palabras clave* — *Disponibilidad, Integridad, Seguridad, API, Searchable Symmetric Encryption (SSE), Reconocimiento Facial, Frame, Passwordless.

I. INTRODUCCIÓN

En la actualidad, casi todas las industrias utilizan tecnología para soportar su modelo de negocio, lo que vuelve necesario que las empresas modernas cuenten con sistemas que digitalicen sus procesos internos, con los cuales ofrecen servicios al público. Como muestra de lo anterior, la siguiente gráfica, tomada directamente del artículo *La digitalización mundial en 10 gráficos* publicado por el Banco Mundial [1], permite observar el comportamiento de la inversión en soluciones digitales en diferentes periodos de 2020, 2021 y 2022:

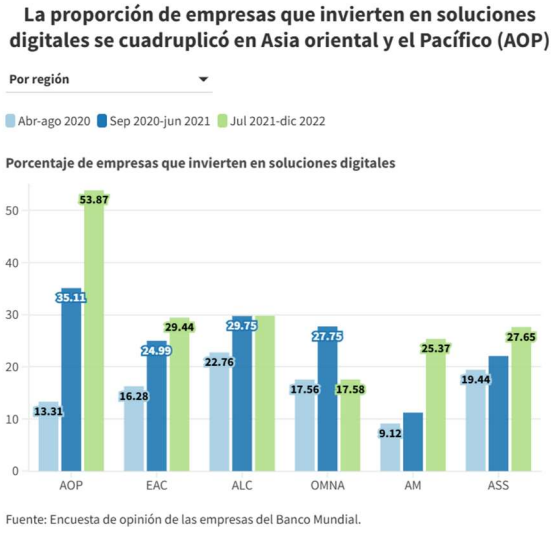

Ilustración 1. Inversión de empresas en soluciones digitales [1].

Adicionalmente, ha habido un aumento generalizado de ataques cibernéticos a nivel mundial este año [2], también ocasionado por los grandes avances en Inteligencia Artificial (IA). Este panorama genera preocupación en empresas cuyos servicios estén basados en la gestión de datos. Lo anterior constituye un problema grave cuando dichos datos son manipulados de manera inapropiada, o si las empresas no cuentan con sistemas suficientemente seguros para garantizar la confidencialidad, integridad y disponibilidad de los mismos, ya que se abre una oportunidad evidente para que personas inescrupulosas roben, modifiquen, secuestren o aprovechen de cualquier manera los datos de una empresa, con el fin de obtener un beneficio económico, o de afectar negativamente a la empresa y sus clientes.

A continuación, se describen dos casos concretos que ilustran la problemática, y donde se evidencia la necesidad de una solución ante dicho problema:

A. En oficinas de abogados, la transferencia de documentos sensibles, como estrategias legales, contratos, evidencias y datos personales de clientes, es una práctica cotidiana. Dicha transferencia puede ocurrir a través de medios electrónicos (correo electrónico, servicios de almacenamiento en la nube, etc.) y en situaciones de trabajo colaborativo. La protección de esta información es crítica no solo para cumplir con normativas de privacidad, como el Reglamento General de Protección de Datos (GDPR), sino también para garantizar la confidencialidad frente a posibles interceptaciones durante la transmisión o accesos no autorizados. En particular, las firmas (o bufetes) de abogados representan un blanco interesante para los atacantes, ya que tienen acceso a información confidencial sobre sus clientes y negocios y porque, en muchos casos, no les es posible costear un buen sistema de gestión de archivos debido a un presupuesto limitado, o a que no consideran que sea una prioridad hacerlo. Esto se ve reflejado en el informe “Legal Survey Report” de 2021 de la American Bar Association, en donde se reveló que una cuarta parte de los bufetes de abogados que fueron encuestados había sufrido filtraciones de datos en algún momento [3].

B. En videojuegos donde un jugador actúa como anfitrión (*host*), los archivos de guardado, que contienen información del progreso de la partida, deben transferirse a otros jugadores en caso de que el anfitrión no esté disponible. Este proceso es esencial para garantizar la continuidad del juego, pero puede presentar riesgos como pérdida, corrupción o exposición de los archivos. Adicionalmente, no es fácil garantizar la

disponibilidad de los archivos de guardado de partida, lo que resulta en la pérdida del progreso de la sesión.

La justificación del problema anteriormente descrito está basada en que la gestión ineficaz de la información crítica en diversos contextos puede afectar negativamente la eficiencia operativa y la toma de decisiones, así como plantear desafíos importantes para la arquitectura de sistemas, la seguridad de datos y la escalabilidad de las soluciones implementadas. Las organizaciones en sectores como el de videojuegos y el legal se beneficiarían enormemente de una solución que garantice la disponibilidad continua y la integridad de los datos críticos. Por ejemplo, en un bufete de abogados un abogado "A" trabaja en un caso con un abogado "B". Ambos necesitan acceder a documentos legales críticos. Actualmente, comparten archivos por correo electrónico o unidades USB, lo que no garantiza su seguridad ni evita el acceso no autorizado. Si uno de los equipos es robado o hackeado, los datos confidenciales pueden ser comprometidos, exponiendo al bufete a demandas legales o pérdidas económicas. Debido a lo anterior, identificamos como problemas principales la ausencia de cifrado en los medios de comunicación, la dependencia de un punto único de acceso a la información y la imposibilidad de rastrear accesos o cambios en los archivos compartidos.
Por lo tanto, se identifican las siguientes necesidades:

- Transmisión Segura: Los abogados necesitan un canal de comunicación que garantice el cifrado de extremo a extremo para la transmisión de datos confidenciales.
- Control de Acceso: Es necesario implementar autenticación y permisos diferenciados para garantizar que solo los usuarios autorizados puedan acceder a los documentos compartidos.
- Disponibilidad Redundante: El sistema debe ser capaz de sincronizar automáticamente los datos en diferentes máquinas o ubicaciones, eliminando la dependencia de un único punto de acceso a la información.

Para lograr cubrir las necesidades, se propone entonces desarrollar un sistema de gestión eficiente para garantizar la disponibilidad continua, el control de acceso, mantener la integridad, confidencialidad y la sincronización de información crítica en entornos distribuidos. Este sistema permitirá a los usuarios acceder y compartir datos de manera segura y sin interrupciones, independientemente de la ubicación o los fallos en los sistemas, mejorando así la continuidad operativa y la toma de decisiones informadas en diversos contextos, haciendo énfasis en los casos presentados para el contexto legal y el de videojuegos.

Para ello, se llevó a cabo el levantamiento de los siguientes requerimientos funcionales:

Nombre	Resumen
RF1	Un usuario podrá registrarse él mismo de forma automática. El sistema realizará las verificaciones necesarias y le indicará el resultado de la operación.
RF2	El sistema debe implementar reconocimiento facial como método de autenticación, para que elimine la necesidad de contraseñas tradicionales, y garantice una autenticación más segura y conveniente (autenticación *passwordless*).
RF3	El sistema debe sincronizar (cargar y descargar) automáticamente los archivos nuevos.
RF4	El sistema debe permitir la creación de grupos entre usuarios, para restringir la sincronización de los archivos.
RF5	El sistema debe permitir la transferencia de archivos entre usuarios de un mismo grupo.
RF6	El sistema debe ofrecer la opción de realizar la sincronización de los archivos manual o automática.
RF7	El sistema debe restringir el acceso al estado del archivo solo a los usuarios autorizados.
RF8	El sistema debe cifrar los datos de los archivos antes de cargarlos.
RF9	El sistema debe almacenar los archivos después de que estos hayan sido cifrados.
RF10	El sistema debe permitir realizar búsquedas sobre los datos cifrados (*Searchable Symmetric Encryption - SSE*).

Tabla 1. Requerimientos funcionales del sistema.

II. DISEÑO DE LA SOLUCIÓN

A continuación, se mostrará y explicará el diseño utilizado para la implementación de la solución:

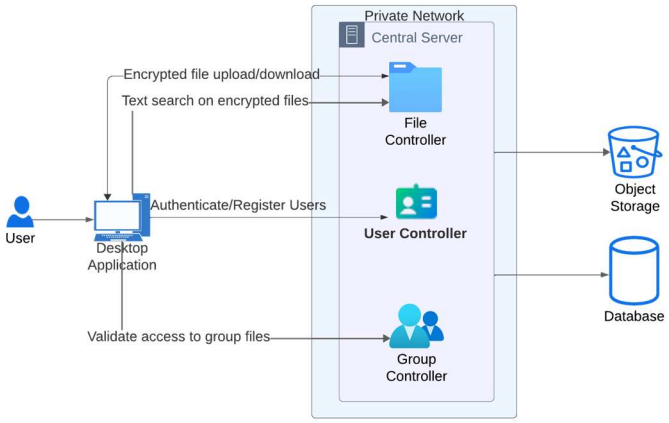

Ilustración 2. Diseño de la solución

El sistema cuenta con los siguientes componentes:

- **Aplicación Principal** (aplicación de escritorio):

  Permite brindar al usuario una interfaz gráfica para que este pueda hacer uso de las funcionalidades del sistema, como iniciar sesión o registrarse, interactuar con los archivos (carga y descarga), realizar búsquedas sobre los archivos cifrados y gestionar los grupos que ha creado, o de los que es parte.

- **Servidor Central**: Cuenta, a su vez, con tres controladores:

  - **Controlador de archivos**: Contiene la lógica de negocio para que el sistema pueda realizar las tareas relacionadas a los archivos. Entre dichas tareas se encuentran: cifrar, cargar y descargar archivos hacia/desde el sistema de almacenamiento de objetos, realizar búsquedas sobre los archivos cifrados.

  - **Controlador de usuarios**: Contiene la lógica de negocio para que el sistema pueda realizar las tareas relacionadas a los usuarios. Entre dichas tareas se encuentran: registrar, iniciar sesión, obtener datos de un usuario registrado.

  - **Controlador de grupos de usuarios**: Contiene la lógica de negocio para que el sistema pueda realizar las tareas relacionadas a la gestión de grupos de usuarios. Entre dichas tareas se encuentran: crear un grupo, agregar usuarios a un grupo existente, eliminar usuarios de un grupo existente.

- **Base de datos**: Permite persistir aquella información que es necesaria para cumplir con los requerimientos funcionales establecidos para el sistema. Tareas como, por ejemplo, el registro de un usuario, hacen que sea necesario almacenar los datos proveídos por este (su correo electrónico, nombres y apellidos, etc).

- **Sistema de almacenamiento de objetos**: Permite, como su nombre lo indica, almacenar objetos, que en este caso corresponden a los archivos gestionados por el sistema. Esto hace que operaciones como la carga y la descarga de los archivos sean tareas fáciles de realizar. Lo anterior, se debe a que dicho sistema provee una solución eficiente y escalable para manejar grandes cantidades de datos no estructurados (archivos en cualquier formato).

III. IMPLEMENTACIÓN DE LA SOLUCIÓN

Para la implementación de los componentes del diseño propuesto en la sección anterior, se utilizaron los siguientes *frameworks*:

- Aplicación de escritorio: Microsoft .NET (Windows Forms).
- Servidor Central: Node.js como ambiente de ejecución de JavaScript (back-end) y Express.js como framework para la construcción del *API REST*.

Adicionalmente, la siguiente lista contiene los proveedores externos que permiten operar el diseño:

- Amazon Simple Storage Service (S3) para el almacenamiento de archivos.
- MongoDB para la persistencia de datos.
- Render para el despliegue y hosting del servidor (ambiente de producción).

A. Back-End

La implementación consiste en un *API REST* construido en el servidor Node.js (back-end), el cual es se comunica con la aplicación de escritorio (mediante el uso del protocolo HTTPS) para dar respuesta a los requerimientos identificados. Dicho servidor se comunica, a su vez, con el servicio de almacenamiento *cloud* (*bucket S3*) para poder almacenar o descargar archivos. Finalmente, el servidor se comunica con la base de datos Mongo, con el fin de realizar las consultas necesarias para el correcto funcionamiento de los controladores de usuarios, archivos y grupos.

El proyecto tiene una estructura con archivos separados para funcionalidades específicas. A continuación, se presenta la estructura de carpetas que se utilizó:

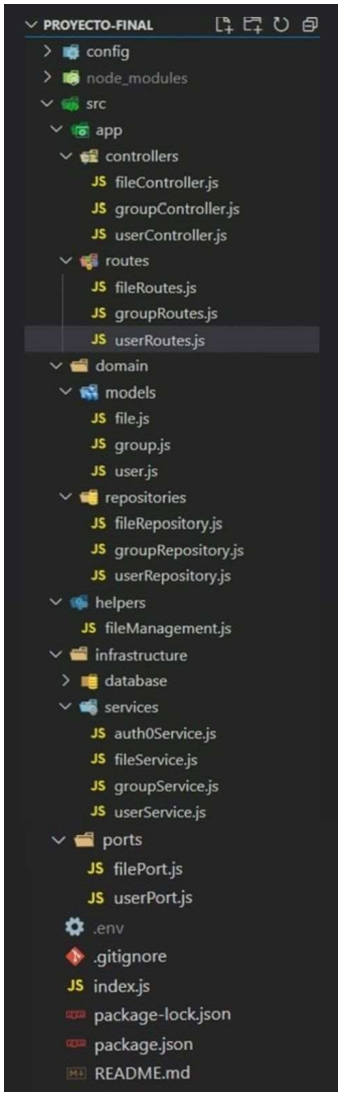

Ilustración 3. Estructura de carpetas del Servidor Central.

La estructura que se puede observar en la *Ilustración 3* corresponde a una arquitectura de puertos y adaptadores (también conocida como arquitectura hexagonal). Se tomó la decisión de utilizarla debido a que facilita el desacoplamiento y permite realizar pruebas de manera efectiva, además de simplificar el reemplazo de componentes, en caso de ser necesario.

B. Aplicación de Escritorio

Para el desarrollo de la aplicación de escritorio, se utilizó *.NET Framework* con el lenguaje de programación C#. La interfaz gráfica fue diseñada y construida empleando Windows Forms, una herramienta versátil y accesible para crear aplicaciones visuales en entornos Windows.

Se cuenta con una ventana principal desde donde se puede registrar un usuario nuevo, o se puede ingresar el email para iniciar sesión:

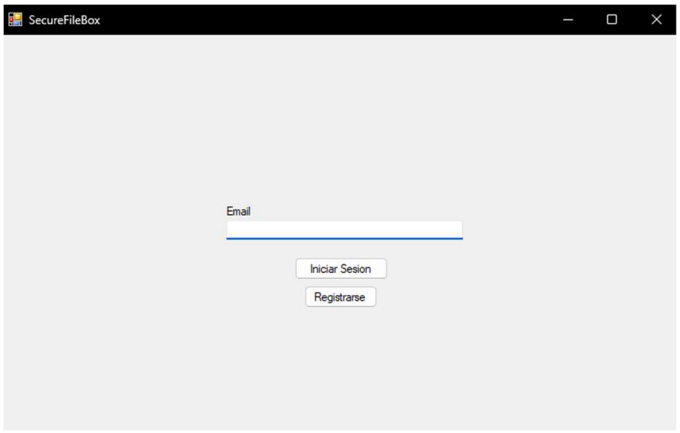

Ilustración 4. Formulario de login

Para el registro de usuarios es necesario el nombre, el apellido, el email, una contraseña y el registro facial del usuario. Para el registro facial, el usuario debe presionar el botón “Capturar Imagen” y deberá mover la cara en diferentes direcciones, mientras se van guardando diferentes posiciones del rostro:

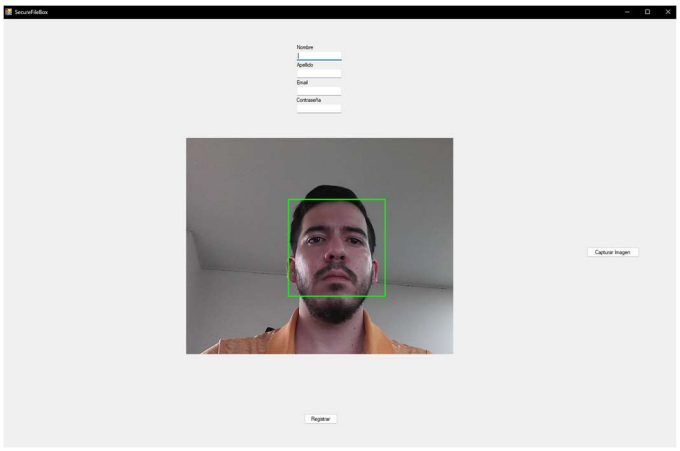

Ilustración 5. Ventana de registro de la aplicación

Para el ingreso, el usuario deberá ingresar su email en la ventana principal, que luego lo redireccionará a otra ventana para hacer la validación del rostro y así autorizar su ingreso. En caso de requerirse (porque el usuario lo desee o se presenten fallos o indisponibilidad del servicio de reconocimiento facial), también se puede hacer el inicio de sesión desde la pantalla que se muestra en la *Ilustración 6*, ingresando la contraseña (*login* tradicional):

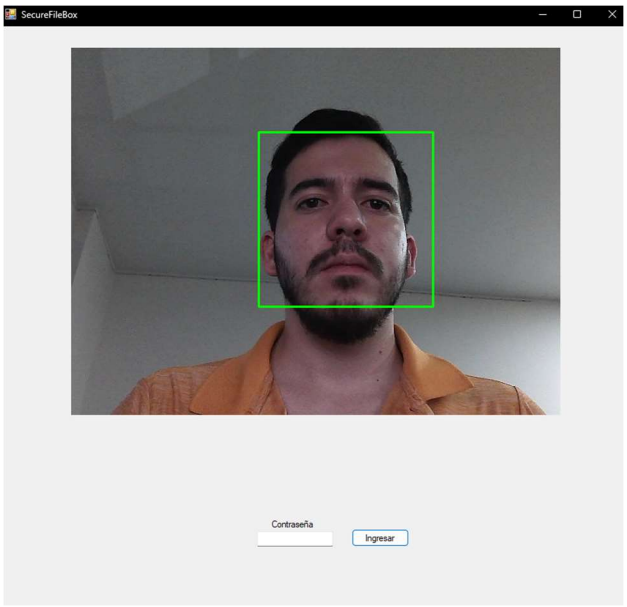

Ilustración 6. Login tradicional

Luego de ingresar, el usuario ve una lista de los grupos de los que es dueño y de los grupos a los que pertenece. También, tiene la posibilidad de crear uno nuevo si lo desea o, si no pertenece a ninguno, para compartir archivos con otros usuarios y empezar a hacer seguimiento de estos:

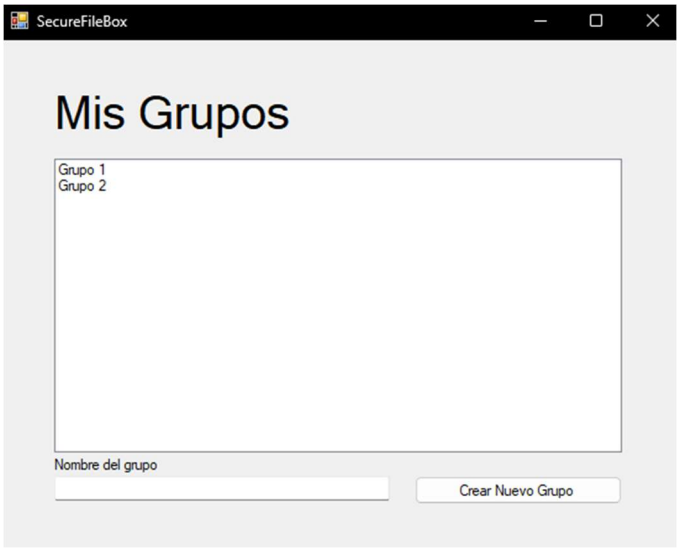

Ilustración 7. Ventana de grupos del usuario

Al seleccionar un grupo e ingresar, el usuario podrá observar los archivos que se están siguiendo para sincronizar y una lista de los usuarios del grupo con su rol, desde allí puede agregar archivos para sincronizar, descargar archivos que estén siendo sincronizados por otro usuario del grupo, realizar búsquedas de archivos por palabras clave y agregar o eliminar usuarios del grupo, y cambiar el rol de estos si es el dueño:

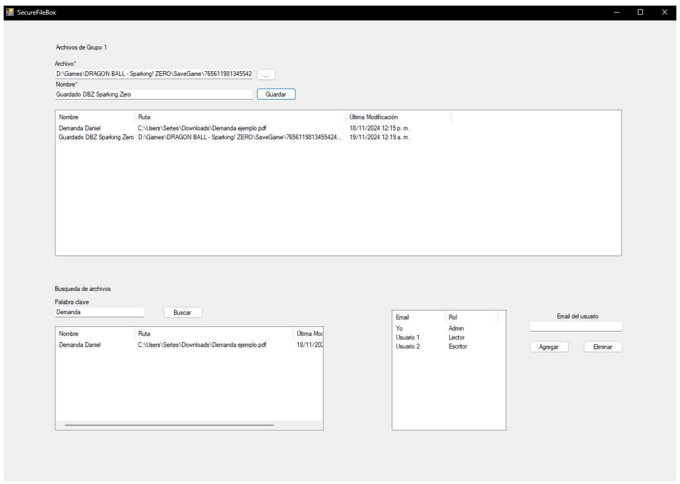

Ilustración 8. Ventana de gestión de archivos de la aplicación

IV. FUNCIONALIDADES DE LA APLICACIÓN

1) Carga y descarga de archivos

Para esta funcionalidad, se utilizó el servicio de almacenamiento de objetos en la nube de AWS: *Simple Storage Service* (o *S3*). Para ello, se creó un *bucket* desde la consola de AWS, en donde se almacenaron todos los archivos que la aplicación debía soportar y gestionar.
La ventaja de utilizar un servicio como este es que permite almacenar cualquier tipo de archivo, incluso bajo una estructura definida de carpetas. Para poder incluir S3 en el servidor, se utilizó el SDK del cliente de AWS *S3* disponible para Node.js.

2) Cifrado de archivos

Para este requerimiento, se cifraron los archivos con el algoritmo *AES-256* (en modo *CBC*), con una llave de cifrado de 256 bits (32 bytes) y un vector de inicialización de 128 bits (16 bytes), que fueron generados con el software *OpenSSL*. El cifrado de datos se logró mediante el uso de la librería *crypto* de Node.js.

3) Autenticación por reconocimiento facial

Para la implementación de un reconocimiento facial como autenticación *passwordless,* se utilizó la librería de Emgu CV que es un *wrapper* de la librería de OpenCV para *.NET* [4].Cuando un usuario se registra se inicia la cámara para capturar *frames* en tiempo real, se utiliza un clasificador Haar Cascade para detectar rostros dentro de los *frames* capturados y se toman 40 imágenes del rostro detectado, recortando la región correspondiente al rostro para poder registrar diferentes perspectivas de la cara. Para ello, el usuario debe mover la cara en diferentes direcciones, con el fin de poder registrar todos los ángulos necesarios.

Luego, se crea un archivo que contiene todas las imágenes, se cifra y se sube al *bucket S3,* bajo el identificador '*biometric/nombre-de-usuario/archivo-de-imágenes.zip*'.
Cuando el usuario desea hacer *login* en la aplicación, se descargan las imágenes del rostro autorizado asociado al usuario al momento de registrarse, las cuales se utilizan para entrenar un modelo de reconocimiento facial basado en *LBPHFaceRecognizer* y se activa la cámara. La cámara captura *frames* en tiempo real, y un clasificador *Haar Cascade* detecta rostros en los *frames*. Los rostros detectados se redimensionan y se comparan con el modelo entrenado. Si se encuentra una coincidencia con el rostro autorizado dentro de un umbral de distancia especificado, se autentica al usuario y se autoriza su ingreso a la sesión.

4) Búsquedas en archivos cifrados

Para este apartado, es importante mencionar que las búsquedas solo funcionan en archivos de texto (documentos), cuyo formato sea PDF, DOCX o TXT. Para llevarlas a cabo, se creó una función de extracción de palabras clave en los archivos, organizándolas por frecuencia, de mayor a menor. Las 20 palabras con mayor frecuencia dentro del documento se toman como palabras clave, para luego cifrarlas creando un *HMAC* para cada una, con el algoritmo *SHA-256*. Después, se crea una lista con los códigos *HMAC,* para almacenarla en la base de datos *Mongo*, creando así un índice de búsqueda. La cantidad de palabras utilizadas para generar el índice es un parámetro variable, que dependerá de la longitud del documento.

Por lo tanto, cuando un usuario realiza una búsqueda en el documento, se procede a cifrar la palabra buscada, y compararla con el índice creado al momento de subir el archivo al *bucket S3.* Si la palabra cifrada coincide con alguna del índice, se retorna el nombre del documento en el cual se dio la coincidencia. De esta forma, se logra realizar una búsqueda sin haber descifrado el contenido del archivo, ni haber dado información más allá del nombre de este.

A continuación, se muestra cómo se registra en Base de Datos la información asociada a un archivo. En este caso, se utilizaron solo las 3 palabras más frecuentes para la creación del índice de búsqueda. También se puede observar el vector de inicialización IV:

Ilustración 9. Información del archivo que es registrada en la Base de Datos

Finalmente, sería posible realizar búsquedas sobre otros tipos de archivos que no sean de texto. Lo anterior, se logra mediante el uso de colecciones de *tags* (en el caso de imágenes, videos o audio) o de *metadata* (para binarios y archivos comprimidos), que permitan categorizar la información más significativa del archivo. Para generar dichos *tags*, se pueden utilizar modelos de *machine learning* y aplicarlos sobre los datos de los archivos multimedia [5] o, en el caso de archivos comprimidos o binarios, extraer la *metadata* que contenga la información más relevante, para así generar un índice de búsqueda apropiado, según sea el caso.

5) Control de acceso

Para el control de acceso a los archivos, se generó un esquema de grupos de usuarios, en donde cada grupo tiene un administrador y varios miembros. Adicionalmente, se cuenta con una estructura de permisos similar a la que utiliza Linux, pero solo para el acceso de escritura y lectura de archivos, mediante el uso de un String con los permisos posibles: *r (read) o rw (read, write)*.

Por lo tanto, en el momento que un usuario va a consultar un archivo, se revisan sus permisos sobre dicho archivo de la siguiente manera:

- Si es *'r'*, quiere decir que el usuario tiene acceso de lectura sobre el contenido del archivo. Se le permite realizar búsquedas sobre los datos cifrados de este (*SSE*).
- Si es *'rw'*, quiere decir que el usuario tiene acceso de lectura y escritura sobre el contenido del archivo. Se le permite realizar búsquedas sobre los datos, descifrar y descargar el contenido del archivo para su modificación.
- Si no tiene permisos asociados (ni *'r'* ni *'rw'*), no se permite realizar ninguna acción sobre el archivo.

A continuación, se puede observar cómo se almacena la información de un usuario y de un grupo en Base de Datos, en donde se puede evidenciar cómo se relaciona a los grupos, y los permisos asociados a los archivos que contengan:

Ilustración 10. Información del usuario que es registrada en la Base de Datos.

Ilustración 11. Información del grupo que es registrada en la Base de Datos.

6) Sincronización automática de archivos

Los archivos son sincronizados automáticamente con el servidor y con los miembros del grupo, esta funcionalidad se basa en la última fecha de modificación del archivo. Para ello, la aplicación está constantemente monitoreando los archivos que están siendo compartidos y, cuando detecta una nueva fecha de modificación, actualiza el archivo en el servidor. Además, cuando la última fecha de modificación guardada en el servidor es mayor a la que tiene el usuario en su sistema, se hace una descarga automática de la versión más reciente del archivo específico.

V. Evaluación

Para evaluar la aplicación se realizaron pruebas de funcionamiento del control de acceso, tiempos de respuesta de la aplicación, funcionamiento del reconocimiento facial y la búsqueda sobre los archivos cifrados y su efectividad para la sincronización de archivos. Se encontró que la aplicación maneja correctamente el control de acceso, solo los usuarios permitidos y autenticados tienen acceso a la información correspondiente. También, se permite la fácil sincronización de los archivos entre usuarios.

Con respecto al reconocimiento facial, se pudieron percibir pequeños problemas al identificar al usuario. Cuando la iluminación de las imágenes al momento de registrarse y de ingresar son muy distintas, el sistema puede tardar o directamente no reconocer al usuario. Además, al utilizar un algoritmo entrenado con Emgu CV [4] y con solo 40 imágenes era posible que el sistema pudiera llegar a confundir a un usuario con otro. Sin embargo, no se llegó a presentar este problema con las pruebas conducidas.

Para la búsqueda sobre archivos cifrados no se observaron problemas mayores más que la dificultad de identificar las palabras clave (*keywords*) más apropiadas de los archivos para poder crear el índice de búsqueda. Por otro lado, con respecto a los tiempos de respuesta, solo se observaron problemas al utilizar cámaras externas para la identificación del rostro tanto en el registro como en el ingreso a la aplicación, en donde el programa tomó hasta 30 segundos para mostrar la ventana de la cámara.

La propuesta de solución presentada aborda un tema crítico sobre la disponibilidad, seguridad y la gestión de información sensible en entornos distribuidos. Con dicha solución, resaltamos varios puntos clave que mejoran esta situación, ya que no solo se resuelve el problema, sino que también se mejora la experiencia del usuario, se facilita la escalabilidad, y se garantiza la seguridad de los datos mediante tecnologías avanzadas de cifrado y autenticación. Estas características hacen que el sistema sea adecuado para aplicaciones en sectores como el legal y el de videojuegos, en los que la integridad y disponibilidad de la información son cruciales.

Cabe destacar de nuestra solución al problema los siguientes elementos: la integración de un sistema de reconocimiento facial para la autenticación y la implementación de un esquema de cifrado simétrico con capacidad de búsqueda (*SSE*), ya que son un avance y un aspecto diferencial significativo respecto a los sistemas tradicionales que dependen de contraseñas. Por otro lado, también se permite que los usuarios puedan realizar búsquedas en documentos cifrados sin descifrar el contenido, lo cual refuerza la privacidad y la seguridad, sin sacrificar funcionalidad mientras que se proporciona una mayor conveniencia para el usuario.

VI. Conclusión y trabajo futuro

La gestión inapropiada de archivos en un contexto legal y de videojuegos multijugador puede resultar en problemas graves para las firmas de abogados y las empresas que desarrollan videojuegos, respectivamente.

En particular, todo lo relacionado a contratos, estrategias legales, evidencias y datos personales de clientes resulta atractivo para cualquier atacante.

De igual forma, el hecho de no tener una experiencia de juego fluida debido a la ausencia del anfitrión en una partida de un videojuego multijugador resulta frustrante para los demás jugadores, ya que pierden el progreso de su partida debido a que no hay garantías de disponibilidad de los archivos de guardado.

El sistema para la sincronización y gestión segura de archivos se desarrolló con el fin de mitigar casos en donde no se garantiza la confidencialidad, integridad ni disponibilidad de estos activos digitales, que resultan ser críticos para cualquier organización que sea parte de los contextos específicos, expuestos a lo largo de este documento. Las tecnologías utilizadas para el desarrollo del proyecto permiten que se tenga garantía de los atributos de seguridad mencionados anteriormente. Por otro lado, les brinda a las organizaciones una herramienta potente para gestionar, de forma organizada y confiable, cualquier tipo de archivo.

Mediante el uso de distintos algoritmos de cifrado como *AES-256 y SHA-256*, búsquedas sobre datos cifrados (*Searchable Symmetric Encryption*), autenticación por reconocimiento facial y un riguroso control de acceso a los archivos, mediante el uso de permisos y grupos, se lograron los objetivos específicos definidos al inicio del proyecto.

Como trabajo futuro, se ve una gran oportunidad en la implementación de la solución en un contexto de banca digital, ya que es una tendencia que ha tomado mucha fuerza durante los últimos años, y en donde es evidente que sería valioso un sistema que permita manejar adecuadamente los datos bancarios de los usuarios, como extractos de productos

financieros, información sobre su perfil de crédito, certificados, etc.

La implementación de la solución en el contexto de banca digital también permitiría mitigar otros factores de riesgo para los clientes, como lo son la suplantación de identidad, o la transferencia no consentida de activos. Así, se brindaría una mayor confianza y tranquilidad a la base de clientes existentes, y se alentaría a clientes potenciales a tener productos financieros con los bancos digitales.

BIBLIOGRAFÍA

[1] Banco Mundial, "La digitalización mundial en 10 gráficos", *Banco Mundial*, 5 de marzo de 2024. [En línea]. Disponible en: https://www.bancomundial.org/es/news/immersive-story/2024/03/05/global-digitalization-in-10-charts.

[2] CrowdStrike, "Infografía: Informe de amenazas globales 2024" *CrowdStrike*, febrero de 2024. [En línea]. Disponible en: https://www.crowdstrike.com/wp-content/uploads/2024/02/gtr-2024-infographic_es-LA.pdf.

[3] Wolters Kluwer, "Ciberseguridad para bufetes de abogados" *Wolters Kluwer,* 23 de junio de 2023, [En línea]. Disponible en: https://www.wolterskluwer.com/es-es/expert-insights/cybersecurity-for-law-firms.

[4] Emgu CV, "Emgu CV: OpenCV in .NET", *Emgu CV,* [En línea]. Disponible en: https://www.emgu.com/wiki/index.php/Main_Page.

[5] Microsoft Learn, “Index file content and metadata by using Azure AI Search”, *Microsoft Learn,* [En línea]. Disponible en: https://learn.microsoft.com/en-us/azure/architecture/ai-ml/architecture/search-blob-metadata