Muyal-Chimalli: Servicio para el acceso seguro y confiable a datos sensibles

Diana E. Carrizales-Espinoza[1[0000-0002-3925-031X]], J.L. González-Compeán[1[0000-0002-2160-4407]], Miguel Morales-Sandoval[1[0000-0003-1702-8467]], y Ricardo Marcelín-Jiménez[2[0000-0002-5355-5830]]

[1] Cinvestav Tamaulipas, Cd. Victoria, México
[2] UAM-Iztapalapa, Cd. México, México
diana.carrizales@cinvestav.mx, joseluis.gonzalez@cinvestav.mx, miguel.morales@cinvestav.mx, rmarcelin@izt.uam.mx

Resumen. La producción de datos ha aumentado de forma exponencial en los últimos años debido, entre otras razones, al incremento de dispositivos IoT (p. ej., electrocardiogramas y sensores) y dispositivos de usuario final (p. ej., celulares y tabletas). De esta forma, los datos generados son almacenados en diferentes ubicaciones geográficas durante todo su ciclo de vida. Lo anterior, provoca una gestión jerárquica que permite producir una respuesta rápida al analizar, preservar o transportar un gran volumen de datos (*big data*). La nube se ha vuelto de vital importancia para gestionar esta gran cantidad de datos; sin embargo, es necesario contar con mecanismos que permitan asegurar, preparar, entregar y recuperar datos sensibles de forma segura, confiable y eficiente en escenarios reales donde estos datos son clave para la toma de decisiones (p. ej., los del ámbito médico, tales como expedientes clínicos y tomografías). En este capítulo se presenta Muyal-Chimalli, una herramienta computacional conformada por un conjunto de servicios que permiten a las instituciones de salud, profesionales de salud, pacientes y/o comunidad científica acceder a los servicios de e-salud y/o sistemas de analítica para asegurar el manejo, preparación y acceso seguro y confiable de datos sensibles. Muyal-Chimalli verifica, automáticamente y de forma transparente, que cada sistema de e-salud observe las normas nacionales e internacionales, garantizando la privacidad, confidencialidad, integridad y disponibilidad de los contenidos, así como estableciendo tolerancia a fallas de servicios/servidores y creando registros inmutables en una red privada (blockchain) para brindar trazabilidad al manejo de los datos.

Palabras clave: Seguridad Informática · Confiabilidad y Eficiencia de Datos · Trazabilidad · Datos Sensibles · Sistemas de e-Salud y Analítica.

1 Introducción

En los últimos años se ha observado un incremento exponencial en la producción de los dispositivos de IoT (p. ej., sensores, electrocardiogramas, tomógrafos, espirómetros) [1]. En consecuencia, el volumen de los datos producidos y gestionados por las organizaciones también ha aumentado [2]. Lo anterior se debe a que los usuarios finales que se encuentran asociados a dichas organizaciones producen, almacenan, intercambian y utilizan los datos constante y continuamente, provocando, así, un efecto de acumulación de datos [3].

En escenarios reales, esta tendencia da como resultado un procesamiento de grandes volúmenes de datos conocido como *big data*. En estos escenarios, grandes repositorios de datos son producidos de forma continua por los dispositivos de IoT (es decir que se genera un gran *volumen* de datos) para obtener información útil que será utilizada como entrada (información *veraz* que tiene *valor* para un grupo de personas y/u organizaciones) en procesos críticos de toma de decisiones (los cuales necesitan realizase con la mayor *velocidad* posible debido a la sensibilidad de dichos procesos) [4], [5].

De esta forma, los datos generados son almacenados en diferentes ubicaciones geográficas durante todo su ciclo de vida. La Figura 1 muestra una representación conceptual del ciclo de vida de los datos, el cual incluye la adquisición, el indexamiento, pre-procesamiento, análisis, uso, compartición y el consumo de los datos.

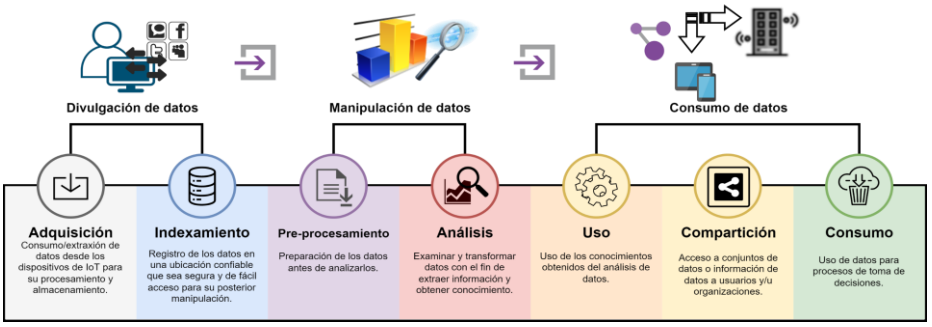

Figura 1. Representación conceptual del ciclo de vida de los datos.

Convencionalmente, el cómputo en la nube [6] ha sido la solución más popular para el procesamiento y almacenamiento datos producidos desde los dispositivos de IoT y de usuario final (p. ej., celulares, tabletas, laptops, estaciones de trabajo, etc.) [7]. De la misma forma, el cómputo en la nube se ha convertido en un soporte para escenarios de big data [8], [9]. No obstante, a medida que los sistemas que almacenan estos datos escalan y la producción de datos aumenta, la recopilación, la gestión y el procesamiento de datos de forma centralizada se vuelve inviable.

Además, es importante considerar que, en los distintos entornos organizacionales, como lo son los hospitales, es necesario procesar, preservar y compartir

datos sensibles con otras organizaciones de forma segura, confiable y rentable. Para dicho fin se han establecido distintos requisitos no funcionales obligatorios, impuestos por las leyes en cada país, a través de normas (p. ej., NOM-024-SSA3-2010 y NIST) y protocolos (p. ej., DICOM/HL7) para el intercambio y preservación de datos sensibles que es necesario que las organizaciones cumplan. Estos requisitos van desde la seguridad de los datos durante su transporte y almacenamiento, hasta el establecimiento de controles de acceso a los datos (es decir, privacidad) y el aseguramiento de la integridad y la confidencialidad de estos, así como su confiabilidad.

Debido a estos factores, ha surgido la necesidad de contar con servicios que permitan mantener, transportar y procesar datos sensibles de forma segura, eficiente y confiable. En este capítulo se presenta Muyal-Chimalli, una herramienta computacional conformada por un conjunto de servicios que permiten el acceso seguro de datos sensibles en servicios de e-salud y servicios de analítica. La Figura 2 muestra una representación conceptual del uso de Muyal-Chimalli en un escenario real de transporte y preservación de datos sensibles.

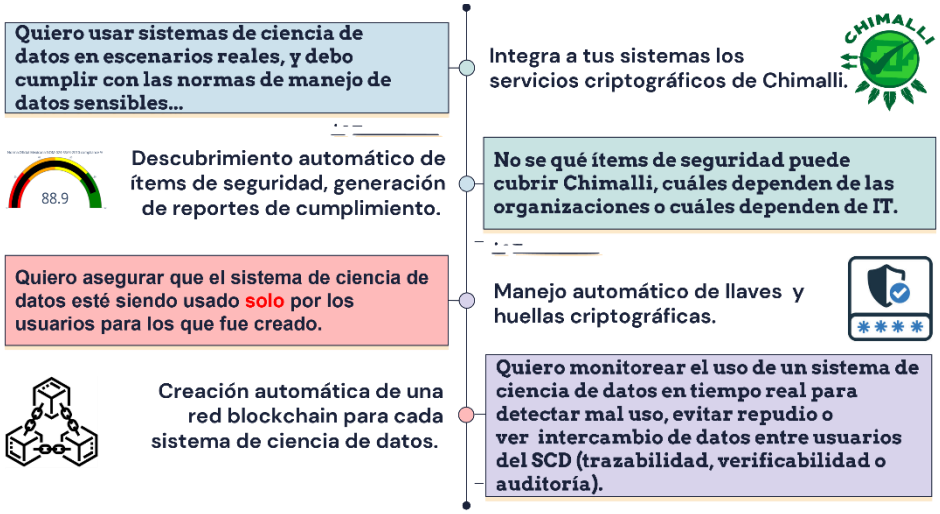

Figura 2. Representación conceptual de la descripción general del uso de Muyal-Chimalli.

Muyal-Chimalli se encuentra compuesto por un conjunto de servicios para acceder, manejar, preparar, transportar y recuperar datos médicos. Estos servicios permiten a las instituciones de salud, profesionales de la salud, pacientes y/o comunidad científica acceder a los datos de forma segura y confiable a través de servicios de e-salud y/o sistemas de analítica para obtener información útil que ayude a mejorar la toma de decisiones en escenarios de salud. Por ejemplo, la Figura 3 muestra una representación conceptual de un escenario donde el médico de un hospital envía una radiografía a un especialista que se encuentra en otro hospital. Dicho proceso debe ser realizado siguiendo los protocolos necesarios para asegurar que los datos sean íntegros, confiables y seguros, además de que sean entregados en el menor tiempo posible.

Figura 3. Representación conceptual de un escenario real de salud crítico para la toma de decisiones.

Las principales características que provee Muyal-Chimalli a los datos son:

- *Confiabilidad y disponibilidad* - garantiza el acceso a los datos, así como a los sistemas de e-salud y analítica en escenarios de fallas de servidores y almacenamiento de datos, así como apagones en los centros de datos; Muyal-Chimalli permite configurar los servicios de confiabilidad y disponibilidad de acuerdo con los recursos disponibles en la organización [10], [11];
- *Eficiencia* - Muyal-Chimalli maneja los datos hasta 10 veces más rápido que opciones disponibles en el mercado; además, permite una reducción del 34% en relación con los costos de utilización de la nube y de un 70% en relación con los costos de almacenamiento; asimismo, Muyal-Chimalli permite compartir sistemas con otras instituciones en minutos y de forma segura (es decir, permite compartir datos de forma intrainstitucional e interinstitucional) [12];
- *Trazabilidad* - crea automáticamente redes de blockchain para auditoría continua durante el intercambio de datos; Muyal-Chimalli elimina los costos derivados de contratar un servicio de blockchain con terceros (p. ej., se estima que se requieren, aproximadamente, $3,400 dólares por 4 meses de uso de la red en la nube) [13];
- *Seguridad* - asegura la *privacidad*, *confidencialidad* e *integridad* de los datos y establece *controles* de *acceso* de forma automática; además, permite la verificación y creación de reportes que muestran el grado de cumplimiento de los protocolos y normas oficiales nacionales e internacionales para el intercambio y almacenamiento de datos sensibles [14], [15].

El objetivo principal de Muyal-Chimalli es proveer, de forma automática y transparente, tolerancia a fallas en TIC (Tecnologías de la Información y la Comunicación), así como privacidad, confidencialidad, integridad, disponibilidad y trazabilidad en datos sensibles para que los sistemas de e-salud y los sistemas de analítica cumplan con las normas nacionales (NOM-024-SSA3-2010, NOM-004-SSA3-2012) e internacionales (NIST, COBIT 5, ISO 27001:2013) para el transporte y preservación de datos.

El resto de este capítulo está organizado de la siguiente forma. La Sección 2 presenta una descripción detallada sobre el servicio de acceso seguro a los servicios de e-salud y/o servicios de analítica; de la misma manera, se describen

los componentes que lo conforman. La Sección 3 describe los principales resultados obtenidos al utilizar Muyal-Chimalli en servicios de e-salud y/o analítica de datos. Finalmente, la Sección 4 concluye este trabajo dando un resumen sobre el servicio presentado en este capítulo.

2 Servicio de acceso seguro a servicios de e-salud y/o sistemas de analítica

La palabra Muyal proviene del glifo maya que significa "nube en el cielo" (ver Figura 4), mientras que la palabra Chimalli proviene del náhuatl y significa *escudo* (ver Figura 4), el cual era un objeto defensivo utilizado por las fuerzas militares prehispánicas mesoamericanas. De esta manera, Muyal-Chimalli hace referencia a un *escudo en la nube*, el cual permite proteger los datos, ya sea para su transporte o preservación.

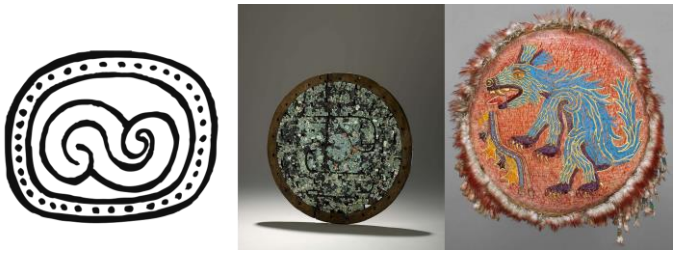

Figura 4. Representación maya de Muyal y ejemplos de dos chimallis utilizados en la antigua Mesoamérica.

Muyal-Chimalli es una herramienta computacional conformada por un conjunto de servicios que permiten a las instituciones de salud, profesionales de la salud, pacientes y/o comunidad científica acceder de forma segura a datos sensibles a través de servicios de e-salud y/o sistemas de analítica. Para este fin, Muyal-Chimalli cuenta con *esquemas* que permiten la *preparación* y *recuperación* de los datos, así como *mecanismos de control de acceso*.

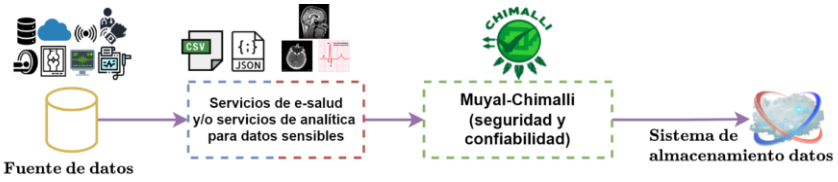

Figura 5. Representación conceptual de un flujo de datos de un sistema de e-salud y/o un sistema de analítica utilizando Muyal-Chimalli para proveer seguridad a los datos.

Muyal-Chimalli garantiza que los datos y los tomadores de decisiones reúnan las condiciones para realizar procesos de análisis. Además, permite la validación y el registro de cualquier operación de compartición de datos que sea realizada dentro de los sistemas de e-salud y/o los sistemas de analítica. La Figura 5

muestra una representación conceptual del flujo de datos de un sistema utilizando los servicios de Muyal-Chimalli para proveer seguridad a los datos.

Muyal-Chimalli permite alcanzar un porcentaje de hasta el 70% en el cumplimiento de las normas y protocolos estandarizados de forma nacional e internacional referentes al manejo, intercambio y transporte seguro y confiable de datos sensibles. Es importante considerar que el porcentaje restante que no es posible cubrir con los servicios de Muyal-Chimalli corresponde a aquellas actividades que necesitan ser realizadas de forma manual por el personal de TI de una organización/institución, o que no pueden ser realizadas por un servicio tecnológico (p. ej., la generación de llaves públicas y privadas, la cual necesita ser realizada por una entidad de confianza). Además, Muyal-Chimalli permite cubrir todas las fases de interconexión establecidas por las normas oficiales (NOM-024-SSA3-2010, NOM-004-SSA3-2012, ISO 27001:2013, COBIT 5 y NIST).

En este sentido, las normas nacionales NOM-004-SSA3-2012 y NOM-024-SSA3-2010 establecen tantos los objetivos funcionales y las funcionalidades que es necesario que los sistemas observen para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros en salud, así como el establecimiento de los distintos criterios científicos, éticos, tecnológicos y administrativos en la elaboración, integración, uso, manejo, archivo, conservación, propiedad, titularidad y confidencialidad de los expedientes clínicos [16]. Por otra parte, las normas internacionales COBIT 5, NIST e ISO 27001:2013 establecen el marco de trabajo para la gestión de los sistemas de seguridad de la información, así como la gestión de las tecnologías de la información para proporcionar confidencialidad, integridad, seguridad y disponibilidad de forma continua, así como el cumplimiento legal de ésto [17].

Para este fin, Muyal-Chimalli crea un reporte/resumen de seguridad, el cual permite revelar las tareas de ciberseguridad (práctica de proteger los sistemas e información de los ataques digitales) que dependen de actividades realizadas por el personal de la salud para que las instituciones puedan crear un plan para implementarlas. Además, asegura tanto la confidencialidad como el anonimato mediante el uso de técnicas de cifrado, las cuales son aplicadas a los datos entrantes y salientes de los sistemas de e-salud y/o los sistemas de analítica. También, permite detectar si surge alguna alteración en los datos (corrupción de datos), asegurando la integridad de éstos. De la misma forma, permite realizar automáticamente la gestión de contratos inteligentes y de transacciones (los procesos, etapas y usuarios por las cuales pasaron los datos), así como la verificabilidad de estas de forma confidencial.

Los componentes principales de Muyal-Chimalli son los siguientes:

- Servicios para la *preparación* y *recuperación* de datos sensibles - dichos servicios son configurables, e incluyen métodos, algoritmos y técnicas para brindar los requisitos de *seguridad*, *trazabilidad*, *integridad* y *eficiencia*;
- Mecanismos de *trazabilidad y verificabilidad* de datos basados en blockchain - permiten registrar todos los procesos, etapas y usuarios por los que han pasado los datos;

- Mecanismos de *control de acceso* de usuarios - aseguran que solo aquellos usuarios/organizaciones que tengan el debido acceso a los datos puedan acceder a ellos;
- Servicios de *validación* de normas oficiales nacionales e internacionales y protocolos DICOM/HL7 - permiten la generación de reportes de cumplimiento de las normas y protocolos;
- Un servicio que permite la utilización de técnicas de criptografía de siguiente generación [18] para la transformación de datos en objetos seguros - permite mantener la *integridad* y *confidencialidad* de los datos.

2.1 Servicios de preparación y recuperación de datos médicos configurables que proveen seguridad, trazabilidad, integridad y eficiencia a los datos

En escenarios reales de gestión de datos sensibles, es necesario contar con mecanismos que provean requisitos no funcionales (un requisito que especifica los criterios que se pueden utilizar para juzgar el funcionamiento de un sistema, en lugar de comportamientos específicos), tales como seguridad, eficiencia y confiablidad. Estos requisitos son necesarios debido a las normas de gestión de datos sensibles (por ejemplo, las normas oficiales mexicanas NOM-004-SSA3-2012 y NOM-024-SSA3-2010) y a las leyes impuestas por los gobiernos y organizaciones [19], [20].

En esta subsección se presenta una descripción de los esquemas de *preparación* y *recuperación* de datos, los cuales permiten el manejo de los requisitos no funcionales. En este sentido, dicha *preparación* de datos es realizada antes de que los datos sean transportados a través de un flujo de datos (cargados para su preservación o compartidos a través de entornos no controlados, como lo es la nube [21]). Para ello, primero se presenta una descripción de la estructura de procesamiento de tuberías. Dicha estructura permite crear los esquemas de *preparación* y *recuperación* de datos y, posteriormente, se realiza una descripción de los requisitos no funcionales que pueden ser incluidos a las tuberías de procesamiento.

Estructura de los esquemas de *preparación* y *recuperación de datos*. En Muyal-Chimalli, la estructura de los esquemas de *preparación* y *recuperación* de datos está construida como tuberías, las cuales se modelan con base en un grafo acíclico dirigido (*DAG*, por sus siglas en inglés *Directed Acyclic Graph*). Los nodos que componen este *DAG* representan los algoritmos que proveen los requisitos no funcionales, mientras que las aristas representan las entradas requeridas por los algoritmos, así como los resultados producidos por ellos. En este sentido, una tubería puede incluir tantos algoritmos, que permitan proporcionar requisitos no funcionales, como sea necesario. Lo anterior permite dar cumplimiento a las normas, protocolos y leyes nacionales e internacionales para la preservación e intercambio de datos sensibles en una misma organización y entre distintas organizaciones (es decir, de forma intrainstitucional e interinstitucional). De este modo, la ejecución sucesiva de los requisitos no funcionales permite la creación de una tubería de procesamiento de datos. La **Figura 6**

muestra una representación conceptual del intercambio de datos entre dos organizaciones utilizando Muyal-Chimalli. En este ejemplo, los datos son extraídos desde la organización A; posteriormente, son registrados en la base de datos y luego son cifrados. Una vez que los datos han sido cifrados, éstos son enviados al servicio de almacenamiento. Después, la organización B podrá acceder a los datos; para ello, el esquema de recuperación realiza el proceso inverso al esquema de preparación. En este caso, los datos primero son descifrados y, posteriormente, se verifica su integridad. Una vez realizado este proceso, los datos son entregados a un usuario perteneciente a la organización B.

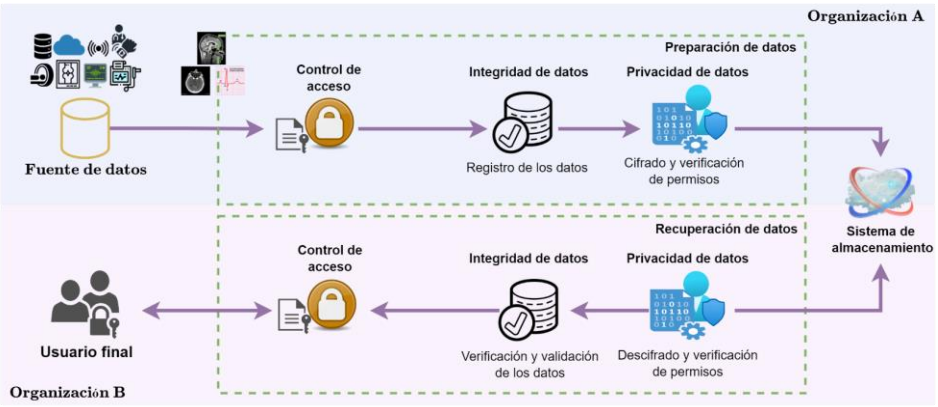

Figura 6. Representación conceptual del intercambio de datos entre dos organizaciones utilizando los esquemas de preparación y recuperación de datos de Muyal-Chimalli.

Los algoritmos que permiten observar los requisitos no funcionales en los flujos de datos son computacionalmente costosos. Lo anterior se debe a que dichos algoritmos añaden retrasos en cada una de las etapas de la tubería que se encuentran definidas en el *DAG*. Para poder mitigar el impacto en el rendimiento que se produce al agregar los requisitos no funcionales para la *preparación* y *recuperación* de datos, los esquemas generados consideran bifurcaciones (es decir, división de tareas en la tubería) para producir paralelismo de datos y procesamiento de tareas concurrentes en cada etapa de la tubería.

En las tuberías, cada etapa invoca a un componente llamado gestor de paralelismo, el cual se encarga de crear clones (trabajadores) de los algoritmos de los requisitos no funcionales a los cuales se les asigna una carga de trabajo. Este gestor también se encarga de desplegar una entidad conocida como balanceador de carga la cual se encarga de mejorar el rendimiento del procesamiento a través de la distribución equitativa (en un sentido estadístico) de los datos/tareas sobre los *trabajadores* habilitados. Este modelo de procesamiento posibilita la producción de un paralelismo implícito que permite la ejecución de los algoritmos de los requisitos no funcionales de forma paralela. Lo anterior, permite reducir el tiempo de preparación y/o recuperación de los datos antes de que sean transportados a través de los flujos de trabajo.

Requisitos no funcionales en los esquemas de *preparación* y *recuperación* de datos. Muyal-Chimalli permite agregar al manejo de datos en los

flujos de procesamiento distintos requisitos no funcionales: i) confiabilidad; ii) seguridad; y iii) costo-eficiencia.

En este sentido, la confiabilidad permite mitigar aquellos problemas causados por deficiencias presentadas en la infraestructura donde los datos se procesan y almacenan [22], [23]. Este requisito se consigue utilizando el conocido algoritmo de dispersión de información (IDA, por sus siglas en inglés *Information Dispersal Algorithm*) [24] . Este algoritmo fue propuesto en 1990 por Michel Rabin y permite dividir/separar/segmentar un archivo en n segmentos (donde n es un número natural), a los cuales se les añade redundancia (es decir, la duplicación o reescritura de información encontrada en el archivo), lo cual permite aumentar la confiabilidad a la hora de recuperar los datos. Dichos segmentos, conocidos como dispersos, son enviados a distintas ubicaciones (de forma distribuida), en donde, para recuperar un archivo, solo se requieren un total de m de ellos (donde m es un número natural y siempre será menor a n) de los n originales. Por ejemplo, con este algoritmo un archivo puede ser transformado en 5 dispersos (n), los cuales serán enviados a 5 ubicaciones distintas. Para recuperar dicho archivo, por ejemplo, solo se requiere acceder a 3 de estas ubicaciones (es decir, permite tolerar 2 fallas) para extraer los dispersos que almacenan (m) y con ellos reconstruir el archivo original. Esto es útil en escenarios distribuidos de datos (como la nube), donde si alguna de las ubicaciones de almacenamiento presenta una falla, el usuario no lo notará, ya que podrá recuperar sus datos accediendo a las demás ubicaciones de almacenamiento donde se colocaron el resto de los segmentos.

Por otro lado, la característica de *seguridad* (en la cual se añade *confidencialidad*, *integridad* y *control de acceso*, CIA, por sus siglas en inglés Confidentiality, Integrity and Access Control), es añadida a los datos para resolver problemas que surjan del transporte y compartición de datos en entornos no controlados y no confiables (por ejemplo, la nube [25], [26]). Esta característica se añade mediante técnicas de criptografía de siguiente generación, como lo es el cifrado basado en atributos.

En estos esquemas, los datos se cifran utilizando el cifrado AES [27] para añadir *confidencialidad*. AES es una función matemática de cifrado conocida como el método de cifrado por bloques (es decir, el cifrado de los datos por medio de algoritmos que permiten convertir un bloque de datos claros en un bloque de datos cifrados a través de una clave) más seguro que existe debido a que, en la práctica, éste no se puede romper, además de que es rápido y eficiente; mientras que, para añadir *controles de acceso*, se utiliza el algoritmo CP-ABE [28], el cual es un cifrado basado en atributos de política de texto cifrado que utiliza árboles de acceso para cifrar datos. En este algoritmo, las claves secretas de los usuarios se generan sobre un conjunto determinado de atributos.

Por otro lado, la *integridad* de los datos se añade generando una huella o firma digital de cada dato. Esta firma/huella es conocida como hash y se centra en lograr dos objetivos: i) la identificación de los contenidos replicados antes de que estos sean enviados al resto de las etapas de *preparación/recuperación* de datos; y ii) la detección de alteraciones en los datos cuando los usuarios descargan/recuperan archivos.

Finalmente, la característica de *costo-eficiencia* se consigue mediante técnicas de compresión y deduplicación de datos. Dichas técnicas permiten reducir el número de contenidos, así como la cantidad de datos a procesar.

Además, estas técnicas permiten reducir el volumen de datos enviados a la nube y, por ende, reducir los costos resultantes de la subcontratación de servicios para realizar las tareas de gestión de datos.

En este sentido, para agregar eficiencia durante el procesamiento de los datos y la ejecución de tareas, se utilizan patrones de paralelismo (es decir, técnicas que permiten realizar tareas o procesar los datos de forma paralela). En Muyal-Chimalli, principalmente se cuenta con dos patrones: i) el patrón manejador/trabajador; y ii) el patrón *divide&vencerás*.

Patrones de paralelismo para la eficiencia en los esquemas para la preparación y recuperación de datos de Muyal-Chimalli. El paralelismo de datos es un paradigma de la programación concurrente. Dicho paradigma consiste en dividir un conjunto de datos y/o tareas de manera que a cada procesador disponible le corresponda un subconjunto de estas tareas/datos.

En este sentido, el patrón *manejador/trabajador* permite procesar los datos en diferentes fases: i) la clonación de tareas; ii) la distribución de tareas y datos; y iii) la supervisión de la ejecución de las tareas.

En la fase de clonación de tareas, el manejador crea instancias de contenedores virtuales (es decir, aplicaciones independientes, empaquetadas con sus dependencias, que pueden ser desplegadas en cualquier entorno sin mayor preparación), los cuales representan clones de una etapa determinada en la tubería del flujo de datos. Los clones creados en esta fase se denominan *trabajadores*.

En la fase de distribución de tareas/datos, el *manejador* lee el contenido almacenado en una fuente de datos y, posteriormente, crea una lista de datos/tareas utilizando un conjunto de rutas. Cada componente de la lista se distribuye de forma balanceada a los *trabajadores* utilizando el algoritmo de balanceo de carga *two choices* [29]. Este algoritmo permite elegir dos trabajadores de forma aleatoria y, posteriormente, escoge el *trabajador* que tenga la menor carga de trabajo [30]. Finalmente, en la fase de supervisión, el *manejador* verifica que los *trabajadores* entreguen los resultados de la tarea realizada a la siguiente etapa en el flujo de los datos.

Por otro lado, el patrón *divide&vencerás* cuenta con tres entidades conocidas como: i) divide; ii) trabajadores; y iii) vences. La entidad *divide* es una instancia de software que se encarga de dividir/segmentar los datos en s segmentos (donde s es un número natural) sin redundancia, los cuales son procesados por los *trabajadores* (similares a los *trabajadores* del patrón *manejador/trabajador*). La entidad *vences* se encarga de consolidar los resultados de cada uno de los *trabajadores* en un único resultado para entregarlo a la siguiente etapa en el flujo de datos.

2.2 Mecanismos de trazabilidad y verificabilidad de datos basados en blockchain de Muyal-Chimalli

La Organización Internacional para la Estandarización (ISO 9001:2008) define la *trazabilidad* como aquella propiedad del resultado del valor de un estándar determinado (donde éste puede estar relacionado con distintas referencias específicas). Usualmente, estos estándares se refieren a normas nacionales o internacionales a través de una cadena continua de comparaciones [31]. Por otro

lado, el comité de seguridad alimentaria de AECOC define la *trazabilidad* como aquel conjunto de procedimientos preestablecidos y autosuficientes que permiten conocer detalles de un producto (como lo es el histórico, la ubicación y la trayectoria) a lo largo de una cadena de suministro en un momento dado, a través de herramientas determinadas [32].

En Muyal-Chimalli, el proceso de *trazabilidad* de datos juega un papel importante dentro de los flujos de trabajo. Lo anterior se debe a que este proceso brinda la posibilidad de identificar el origen de los datos/procesos, así como las distintas etapas por las que han paso los datos a lo largo de todo su ciclo de vida (adquisición, proceso productivo, distribución y logística, hasta llegar al consumidor final) [33], [34].

Este proceso cumple una parte fundamental dentro de Muyal-Chimalli debido a que permite que cualquiera de las entidades involucradas (p. ej., organizaciones, usuarios finales, etc.) puedan acceder a la información de cada una de las etapas por las cuales ha pasado el contenido digital. Lo anterior, permite verificar si se han cumplido con las acciones pactadas, así como conocer si los datos han sido procesados por las entidades correctas. Esto, posibilita aceptar o rechazar los datos con base en la información del flujo de datos (conocida como *traza*), apoyando, de esta forma, la toma de decisiones y mejorando la confianza en el resultado obtenido. En Muyal-Chimalli, este servicio tiene como objetivo asegurar el registro inmutable de cada acción realizada sobre cada activo digital que es procesado en las diferentes cadenas de valor (flujos de datos) generadas a través de los servicios de construcción de sistemas de e-salud y/o sistemas de analítica de datos sensibles.

El mecanismo de *trazabilidad* de Muyal-Chimalli provee las características de *trazabilidad* y *verificabilidad* a cada uno de los productos/datos que se procesan en cualquiera de los servicios de e-salud y/o analítica de datos sensibles. Además, este mecanismo permite realizar *trazabilidad* de forma interna y externa (es decir, dentro de una misma institución, así como colaboraciones entre varias instituciones/organizaciones) de los productos digitales que son procesados y gestionados a través de los sistemas de e-salud y/o analítica.

La tecnología de blockchain de Muyal-Chimalli permite preservar y compartir los datos de forma segura y transparente sin un órgano central de control. Esta tecnología utiliza una base de datos que es segura y que será compartida solo por aquellos usuarios autorizados. De esta forma, es posible comprobar la validez de cada uno de los procesos realizados en el flujo de trabajo en cada una de las etapas.

El servicio de trazabilidad hace uso de las siguientes herramientas para su correcto funcionamiento: i) *Sawtooth* (solución empresarial para construir, implementar y ejecutar redes y aplicaciones de contabilidad distribuida [35]); ii) *Docker* (proyecto de código abierto que automatiza el despliegue de aplicaciones dentro de contenedores de software [36]); y iii) *Docker Compose* (herramienta para definir y ejecutar aplicaciones Docker de varios contenedores, creando una red virtual que permite la comunicación entre ellos de forma eficiente y simple [37]). Además, Javascript es utilizado como lenguaje principal y MySQL como gestor de base de datos.

Lo anterior quiere decir que la blockchain provee diversas ventajas en el sector de cadenas de suministro (conjunto de actividades, instalaciones y medios

de distribución necesarios para llevar a cabo un proceso [38]), el cual se usa como enfoque en Muyal-Chimalli.

2.3 Servicio para la transformación de datos en objetos seguros mediante el uso de técnicas de criptografía de siguiente generación

Debido al crecimiento acelerado de datos que se ha presentado en los últimos años, el cómputo en la nube se ha convertido en el nuevo núcleo de vida de los datos. Incluso, se espera que, en los próximos años, el 49% de los datos se almacenen en la nube pública [39]. Para evitar incidentes o mitigar riesgos que aún ocurren en la nube, como lo son las alteraciones de los datos [40], la pérdida de privacidad, las violaciones de seguridad o los accesos no autorizados a los datos, las organizaciones deben contar con sistemas o servicios que permitan entregar/recuperar los datos de forma segura, confiable y transparente [41].

En este contexto, Muyal-Chimalli cuenta con un servicio para la construcción eficiente de sistemas de seguridad que permiten a las organizaciones compartir, intercambiar y rastrear información en la nube. En este servicio, los sistemas de seguridad y el software de blockchain se convierten en servicios independientes y autónomos. Para mejorar la eficiencia de los servicios de seguridad, así como la experiencia de los usuarios finales, se agregan patrones de paralelismo implícitos junto con técnicas de balanceo de carga a los servicios.

Este servicio permite a las organizaciones respaldar patrones de intercambio de información en línea entre múltiples participantes al acoplar distintos servicios para cumplir con múltiples combinaciones de requisitos de seguridad (p. ej., confidencialidad, integridad, no repudio, autenticación y trazabilidad). Las características principales de este servicio son: i) flexibilidad; y ii) eficiencia.

La *flexibilidad* permite integrar (en un único sistema integral), sobre la marcha y bajo demanda, tantas aplicaciones de seguridad como inquietudes sean expresadas por las organizaciones (etapas en un flujo de datos) y por los participantes de cada flujo de trabajo organizacional. En este método, las aplicaciones de seguridad y el software se convierten en servicios en la nube independientes y autónomos. Este conjunto de servicios se combina para crear sistemas de seguridad en la nube que permiten admitir flujos de trabajo organizacional en línea y que incluyen a varios participantes. En este sentido, un *framework* (estructura que se puede aprovechar para desarrollar un proyecto) basado en este método, permite la creación de sistemas de seguridad en la nube que aseguran el cumplimiento de múltiples requisitos no funcionales de seguridad.

Por otro lado, la *eficiencia* se obtiene utilizando un modelo de programación paralela para la gestión de datos basado en la combinación de patrones de paralelismo, así como de esquemas de balanceo de carga (integrados en las aplicaciones de seguridad). A partir de este modelo se crearon dos esquemas de patrones paralelos llamados: i) *pipeline*; y ii) *overlapped*. El esquema *pipeline* combina dos patrones de paralelismo: *pipe&filter* y manejador/trabajador. En este esquema, el primer patrón es utilizado para organizar las aplicaciones de seguridad en forma de tuberías y el segundo patrón se encarga de desplegar las tuberías creadas en forma de *trabajadores* para ejecutarlas en paralelo. Este esquema se encarga de cifrar/descifrar pequeños conjuntos de datos en paralelo. Por otro lado, el esquema *overlapped* permite el acoplamiento de aplicaciones

de seguridad independientes para que se ejecuten de forma suprapuesta. De la misma forma, permite que aquellas aplicaciones de seguridad que cuentan con algún tipo de dependencia se acoplen en forma de tubería. Este esquema se encarga de cifrar/descifrar grandes conjuntos de datos en paralelo.

Los componentes principales de este servicio son dos: i) un método de seguridad múltiple en la nube para la creación de servicios de gestión de la seguridad de los datos de forma confidencial, flexible, integral y eficiente; y ii) los esquemas de paralelismo (*pipeline y overlapped*) que permiten mejorar el rendimiento de los sistemas de seguridad en la nube, así como el mejoramiento de la experiencia de servicio de los usuarios finales de Muyal-Chimalli.

2.4 Mecanismos de control de acceso de usuarios de Muyal-Chimalli

Para poder cumplir con los requisitos de seguridad en Muyal-Chimalli, se creó un repositorio de aplicaciones de seguridad. Dicho repositorio cuenta con un conjunto de aplicaciones disponibles para que los usuarios finales puedan incluirlos en sus sistemas de seguridad.

Este repositorio cuenta con distintas aplicaciones de seguridad, como lo son los criptosistemas simétricos (estándar de cifrado avanzado, AES [42]), cifrado basado en emparejamiento (firmas cortas) y cifrado basado en atributos (CP-ABE [43]), así como un bloque de trazabilidad que se utiliza para registrar cada transacción de intercambio de información en una cadena de bloques privada [44].

En este contexto, CP-ABE [45] es utilizado para hacer cumplir, criptográficamente, el *control de acceso* de los sistemas de seguridad creados con Muyal-Chimalli. Los criptosistemas basados en emparejamientos, que producen firmas cortas, son utilizados como servicios de autenticación, no repudio e integridad. En Muyal-Chimalli, estos criptosistemas pueden proporcionar cualquier nivel de seguridad equivalente a 128, 192 o 256 bits, los cuales cumplen con la mayoría de los estándares (p. ej., el estándar NIST [46], [47]).

Tanto CP-ABE como las firmas cortas utilizan un emparejamiento bilineal asimétrico que es computacionalmente eficiente. En este sentido, los procedimientos de firma y verificación se implementan utilizando la instancia de la función hash (también conocidas como funciones resumen) SHA3. La combinación de estos algoritmos y funciones da como resultado la adición de distintas propiedades de seguridad a la información.

2.5 Servicios de validación de normas oficiales mexicanas y protocolos DICOM/HL7

En los procesos de preparación/recuperación, transporte y preservación de datos para escenarios reales de gestión de datos sensibles, es necesario considerar distintos requisitos no funcionales (por ejemplo, seguridad, eficiencia y confiabilidad) que ayuden a cumplir con las normas internacionales y nacionales impuestas por los gobiernos y/o las organizaciones que preservan, procesan y comparten estos datos [19], [20].

Para asegurar el cumplimiento de estas normas, regulaciones y leyes, es necesario contar con un servicio que permita la validación de éstos. En este sentido, Muyal-Chimalli cuenta con un servicio que determina el porcentaje de cumplimiento de los flujos de datos creados en los sistemas de e-salud y/o sistemas de analítica con base en las normas internacionales (NIST, ISO 27001:2013 y COBIT 5) y nacionales (NOM-024-SSA3-2010) para la preservación y compartición de datos sensibles. Las principales características de este servicio son: i) preprocesamiento de los datos para leer y manipular los archivos desde el código fuente; ii) identificación de los flujos de trabajo que conforman los servicios de e-salud y/o los servicios de analítica; iii) consulta de las fuentes de información utilizando APIs (interfaz de programación de aplicaciones) para obtener datos y características contextuales de los contenedores, las cuales representan las tareas que ejecuta el contenedor; iv) búsqueda de palabras clave para determinar el cumplimiento de las normas nacionales e internacionales; v) obtención del porcentaje de cumplimiento y generación de un reporte/resumen donde se visualizan los resultados obtenidos durante el análisis del sistema; vi) descubrimiento de los flujos de trabajo asociados con los archivos de configuración del sistema de e-salud y/o sistema de analítica, así como la generación de una representación del DAG obtenido; y vii) verificación de las normas NOM-024-SSA3-2010, NIST, ISO 27001:2013 y COBIT 5 para el intercambio y preservación de datos sensibles.

En este servicio, los archivos de configuración representan el servicio que será desplegado. El programa recibe como entrada los archivos de configuración y determina qué normas nacionales e internacionales cumple dicho servicio. El cumplimiento es mostrado mediante un reporte en donde se especifica el porcentaje de cumplimiento del servicio según las normas correspondientes. Además, el servicio realiza el descubrimiento del flujo de trabajo asociado a los archivos de configuración del servicio de e-Salud y/o servicio de analítica.

Las normas internacionales y nacionales son representadas mediante listas de verificación. Cada lista de verificación contiene los requerimientos de la norma correspondiente. Los requerimientos pueden ser garantizados por el servicio creado (de forma sistemática) o mediante intervención del usuario (es decir, de forma asistida).

El servicio de validación cuenta con cuatro módulos: i) módulo de preprocesamiento para realizar la lectura de los archivos de configuración, los componentes identificados en este módulo son agregados a un diccionario de datos (contiene la lista de claves que cuentan con información sobre los procesos que se realizan en un flujo de datos); ii) módulo de identificación de flujos de trabajo e información de contenedores, el cual permite identificar los flujos, patrones, bloques de construcción, requisitos no funcionales y etapas de procesamientos; iii) módulo de determinación del nivel de cumplimiento de las normas (en este módulo, las normas nacionales e internacionales fueron capturadas de forma manual en una lista de verificación); y iv) módulo de descubrimiento del flujo de trabajo, en el que se genera un DAG, donde las entradas son representadas por los nodos incidentes y las salidas son representadas por los nodos salientes.

3 Principales resultados obtenidos al utilizar Muyal-Chimalli en servicios de e-salud y/o analítica de datos

Muyal-Chimalli provee servicios de seguridad para sistemas de e-salud y/o sistemas de analítica. Estos servicios de seguridad permiten cumplir con los requisitos no funcionales impuestos por las leyes o los gobiernos de cada país, o por las organizaciones donde se realiza este intercambio y preservación de los datos. Se ha comprobado que, mediante el uso de los servicios de seguridad de Muyal-Chimalli, es posible reducir hasta en un 70% los costos del almacenamiento en la nube, así como en el total de datos almacenados al analizar 51 estudios de imágenes médicas. Lo anterior significa una reducción de hasta el 95% del tiempo al transferir los datos a un servicio de almacenamiento y un aumento de 1.52x en la velocidad de transferencia en comparación con una solución tradicional encontrada en el mercado actual (en este caso *Duplicity*, la cual es una solución tradicional para la transferencia de datos que incluye el manejo de duplicados y la compresión de datos) [48], [49].

Los esquemas de costo-eficiencia de Muyal-Chimalli permiten reducir el tiempo de procesamiento de los datos que son enviados a la nube o intercambiados entre distintas organizaciones. Por ejemplo, se comprobó que utilizando los servicios de seguridad de Muyal-Chimalli es posible procesar hasta 100,971 imágenes médicas de formato DICOM en tan solo 42.71 minutos, mientras que procesar esa cantidad de imágenes con una solución tradicional toma alrededor de 432.21 minutos. Lo anterior, implica una reducción del tiempo de procesamiento y un aumento en la velocidad de éste de hasta 10 veces. Además, en Amazon Blockchain (utilizando los servicios de Muyal-Chimalli), por ejemplo, es posible ahorrar hasta un 32% en costos en la trazabilidad de esta cantidad de datos (considerando que, en México, mantener una red de blockchain con un solo empleado y con tan solo cuatro nodos de AWS durante cuatro meses, requiere una inversión aproximada de 8,373.38 dólares) [48].

Los servicios de seguridad informática de Muyal-Chimalli también permiten cumplir hasta en un 70% con las normas NIST, ISO 27001:2013 y COBIT 5, mientras que, sin estos servicios, usualmente los sistemas solo alcanzan hasta un 20% en el cumplimiento de estas normas, ya que solo consideran la tolerancia a fallos. Es importante mencionar que Muyal-Chimalli también permite proporcionar un nivel de seguridad de 256 bits, el cual es el nivel de seguridad más alto recomendado actualmente por el NIST [49].

4 Conclusiones

Los servicios de seguridad informática generados con Muyal-Chimalli permiten a las organizaciones crear servicios de seguridad que se ajusten a sus necesidades y que los ayuden a cumplir con las normas y leyes establecidas por los gobiernos para el intercambio seguro y confiable de datos sensibles. Muyal-Chimalli permite preparar y recuperar los datos, asegurando su confiabilidad, confidencialidad, disponibilidad, anonimato, integridad, trazabilidad y eficiencia. Además, nos permite realizar la gestión automática de contratos inteligentes, así como la verificabilidad de los procesos realizados dentro de un flujo de tra-

bajo de forma confidencial. Debido a lo anterior, Muyal-Chimalli es una herramienta que ayuda a mitigar los riesgos que surgen durante el almacenamiento e intercambio de datos sensibles en procesos críticos para la toma de decisiones.

Agradecimientos

Este trabajo forma parte del proyecto 41756 “Plataforma tecnológica para la gestión, aseguramiento, intercambio y preservación de grandes volúmenes de datos en salud y construcción de un repositorio nacional de servicios de análisis de datos de salud” por FORDECYT-PRONACES.

Referencias

[1] M. A. Malik, "Internet of Things (IoT) healthcare market by component (implantable sensor devices, wearable sensor devices, system and software), application (patient monitoring, clinical operation and workflow optimization, clinical imaging, fitness and wellness measu," Global opportunity analysis and industry forecast, 2014–2021, pp. Allied Market Research, 124, 2016.

[2] J. &. R. D. Gantz, "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east.," IDC iView: IDC Analyze the future, 2007(2012), pp. 1-16, 2012.

[3] . D. Reinsel, J. Gantz and . J. Rydning, "The digitization of the world from edge to core.," IDC White Paper, 2018.

[4] M. Marjani, . F. Nasaruddin, A. Gani, A. Karim, . I. A. T. Hashem, A. Siddiqa and I. Yaqoob, "Big IoT data analytics: architecture, opportunities, and open research challenges," IEEE Access, pp. 5247--5261, 2017.

[5] M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram and S. Raza, "Fog computing: An overview of big IoT data analytics," Wireless Communications and Mobile Computing, 2018.

[6] B. P. Rimal, E. Choi and I. Lumb, "A taxonomy and survey of cloud computing systems," 2009 Fifth International Joint Conference on INC, IMS and IDC, pp. 44--51, 2009.

[7] A. Botta, W. De Donato, V. Persico and A. Pescapé, "Integration of cloud computing and internet of things: a survey," Future generation computer systems, pp. 684--700, 2016.

[8] V. Mosco, "To the cloud: Big data in a turbulent world," Routledge, 2015.

[9] V. Malik and S. Singh, "Cloud, Big Data \& IoT: Risk Management," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), pp. 258--262, 2019.

[10] E. a. A. R. Bauer, "Reliability and availability of cloud computing," 2012.

[11] Y. a. B. C. Izrailevsky, "Cloud reliability," IEEE Cloud Computing, vol. 5, pp. 39--44, 2018.

[12] M. a. A. M. a. F. S. a. N. S. Darbandi, "involving Kalman filter technique for increasing the reliability and efficiency of cloud computing}," in Proceedings of the International Conference on Scientific Computing (CSC), 2012, p. 1.

[13] M. a. M. J. A. a. M.-C. H. M. a. G.-C. J. L. Morales-Sandoval, "Blockchain support for execution, monitoring and discovery of inter-organizational business processes," PeerJ Computer Science, vol. 7, p. e731, 2021.

[14] A. a. A. M. O. a. W. R. a. W. G. Albugmi, "Data security in cloud computing," in 2016 Fifth international conference on future generation communication technologies (FGCT), 2016, pp. 55--59.

[15] G. a. I. M. a. K. F. A. Ramachandra, "A comprehensive survey on security in cloud computing," Procedia Computer Science, vol. 110, pp. 465--472, 2017.

[16] A. a. l. I. y. P. d. D. P. Instituto Nacional de Transparencia, "Recomendaciones para orientar el debido tratamiento de datos personales en los expedientes clínicos de las instituciones de salud pública," 2021.

[17] isotools, "ISO Tools EXCELLENCE," [Online]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Accessed 2022 11 23].

[18] N. A. B. W. J. &. A. R. Gunathilake, "Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications.," in In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019.

[19] H. Mier and T. Delgadillo, "Regulación del acceso al expediente clínico con fines de investigación en México," Revista CONAMED, vol. 22, pp. 27--31, 2018.

[20] Phillips, "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)," Human genetics, vol. 137, pp. 575--582, 2018.

[21] C. B. Tan, M. H. A. Hijazi, Y. Lim and A. Gani, "A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends," Journal of Network and Computer Applications, vol. 110, pp. 75--86, 2018.

[22] Gunawi, Hao, S. O, Laksono, Satria, Adityatama and Eliazar, "Why does the cloud stop computing?: Lessons from hundreds of service outages," SoCC, ACM, pp. 1--16, 2016.

[23] Bala and Chana, "Fault tolerance-challenges, techniques and implementation in cloud computing," International Journal of Computer Science Issues (IJCSI), vol. 9, p. 288, 2012.

[24] R. Marcelín-Jiménez, J. L. Ramírez-Ortíz, E. R. De La Colina, M. Pascoe-Chalke and J. L. González-Compeán, "On the Complexity and Performance of the Information Dispersal Algorithm," IEEE Access, pp. 159284--159290, 2020.

[25] Bhushan and Gupta, "Security challenges in cloud computing: state-of-art," International Journal of Big Data Intelligence, vol. 4, pp. 81--107, 2017.

[26] French-Baidoo, Asamoah and Oppong, "Achieving confidentiality in electronic health records using cloud systems," IJCNIS, vol. 10, p. 18, 2018.

[27] Morales, Gonzalez, Diaz and Sosa, "A pairing-based cryptographic approach for data security in the cloud," IJISP, vol. 17, pp. 441--461, 2018.

[28] Odelu, Rao, Kumari, Khan and Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment," Computer Standards & Interfaces, vol. 54, pp. 3--9, 2017.

[29] M. Mitzenmacher, "The power of two choices in randomized load balancing," IEEE Transactions on Parallel and Distributed Systems, vol. 12, pp. 1094--1104, 2001.

[30] P. Morales-Ferreira, M. Santiago-Duran, C. Gaytan-Diaz, J. Gonzalez-Compean, V. J. Sosa-Sosa and I. Lopez-Arevalo, "A data distribution service for cloud and containerized storage based on information dispersal," SOSE, pp. 86--95, 2018.

[31] iso.org, "ISO 22005:2007(es) Trazabilidad en la cadena de alimentos para alimentación humana y animal — Principios generales y requisitos básicos para el diseño e implementación del sistema," [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:22005:ed-1:v1:es. [Accessed 28 October 2022].

[32] aecoc.es, "AECOC: La Asociación de Fabricantes y Distribuidores," [Online]. Available: https://www.aecoc.es/comite/seguridad-alimentaria/. [Accessed 28 October 2022].

[33] B. a. F. F. a. C. V. a. B. M. a. C. N. a. M. K. Farahani, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," Future Generation Computer Systems, vol. 78, pp. 659--676, 2018.

[34] P. a. A. G. a. G. R. a. C. G. a. F. G. a. L. A. Pace, "An edge-based architecture to support efficient applications for healthcare industry 4.0," IEEE Transactions on Industrial Informatics, vol. 15, pp. 481--489, 2018.

[35] prsarahevans, "Hyperledger Sawtooth: Blockchain para empresas," [Online]. Available: https://prsarahevans.com/cat-guias/hyperledger-sawtooth-blockchain-para-empresas/. [Accessed 2022 11 23].

[36] docker, "Develop faster. Run anywhere.," [Online]. Available: https://www.docker.com/.

[37] D. docs, "docker docs," [Online]. Available: https://docs.docker.com/compose/. [Accessed 2022 11 23].

[38] Banco de México, "Informe Trimestral. Abril-Juno 2021," 2021.

[39] F. Della Rosa, "Worldwide Software as a Service and Cloud Software Forecast, 2020–2024," International Data Corporation (IDC), 2020.

[40] J. a. M. B. a. V. W. Kelly Finnerty and Sarah Fullick and Helen Motha and Navin Shah, Cyber Security Breaches Survey 2019, Department for Digital, Culture, Media and Sport, 2019.

[41] C. H. a. W. C. a. L. Y. a. Y. D. a. S. J. a. Y. T. a. H. C. a. D. Chen, "Toward security as a service: A trusted cloud service architecture with policy customization," Journal of Parallel and Distributed Computing, vol. 149, pp. 76-88, 2021.

[42] J. a. R. V. Daemen, The Design of Rijndael: The Advanced Encryption Standard (AES), Springer Nature, 2020.

[43] M. Morales-Sandoval, J. L. Gonzalez-Compean, A. Diaz-Perez and V. J. Sosa-Sosa, "A Pairing-based Cryptographic Approach for Data Security in the Cloud," Int. J. Inf. Secur., vol. 17, p. 441–461, August 2018.

[44] F. B. a. S. H. a. T. Halevi, "Supporting private data on Hyperledger Fabric with secure multiparty computation," IBM Journal of Research and Development, vol. 63, no. 2/3, pp. 3-8, 2019.

[45] N. a. L. J. a. Z. Y. a. G. Y. Chen, "Efficient CP-ABE Scheme with Shared Decryption in Cloud Storage," IEEE Transactions on Computers, 2020.

[46] D. Giry, "NIST Report on Cryptographic Key Length and Cryptoperiod (2020)," Key length, 2020.

[47] E. a. B. E. a. B. W. a. P. W. a. S. M. a. o. Barker, "Recommendation for Key Management: Part 1-General," National Institute of Standards and Technology, Technology Administration, 2020.

[48] D. S.-G. D. D. G.-C. J. L. &. C. J. Carrizales-Espinoza, "FedFlow: a federated platform to build secure sharing and synchronization services for health dataflows.," Computing, pp. 1-19, 2022.

[49] D. G.-C. J. L. &. M.-S. M. Carrizales-Espinoza, "Zamna: a tool for the secure and reliable storage, sharing, and usage of large data sets in data science applications.," in In 2022 IEEE Mexican International Conference on Computer Science (ENC), 2022, August.

[50] E. a. H. J. J. a. O. A. a. R. D. a. S. G. a. T. H.-Y. Brynjolfsson, "COVID-19 and remote work: An early look at US data," National Bureau of Economic Research, 2020.