Revista científica Sociedad & Tecnología

ISSN: 2773-7349

Fecha de presentación: 25/01/2025, Fecha de aceptación: 28/02/2025, Fecha de publicación: 01/04/2025

Ángel Mauricio Ramón-Noblecilla[1]
E-mail: aramon@utmachala.edu.ec
Orcid: https://orcid.org/0000-0003-4310-8321

Yasser Cesar Alvarado-Salinas[2]
E-mail: yasser.alvarado@instipp.edu.ec
Orcid: https://orcid.org/0009-0009-1945-8576

Johnny Paul Novillo-Vicuña[1]
E-mail: jnovillo@utmachala.edu.ec
Orcid: https://orcid.org/0000-0002-4915-3441

[1]Universidad Técnica de Machala. Machala, Ecuador

[2]Instituto Superior Tecnológico Ismael Pérez Pazmiño, Ecuador

Cita sugerida (APA, séptima edición)

Ramón-Noblecilla, Á. M., Alvarado-Salinas, Y. C., & Novillo-Vicuña, J. P. (2025). Criptografía en la nube: Impacto en la privacidad de las pymes mediante el cifrado homomórfico. *Revista Sociedad & Tecnología*, 8(2), 304-322. DOI: https://doi.org/10.51247/st.v8i2.554.

==== o ====

Criptografía en la nube: Impacto en la privacidad de las pymes mediante el cifrado homomórfico

RESUMEN

Los sistemas criptográficos en la nube, son estudiados en el presente artículo de revisión. Centrándose en el cifrado homomórfico y los sistemas criptográficos parcialmente homomórficos. Se analizan sus aplicaciones, ventajas, limitaciones y tendencias; destacando la capacidad del cifrado homomórfico para procesar datos cifrados, sin necesidad de descifrarlos y exponerlos ante el proveedor de la nube. El enfoque se orienta al uso de tecnologías criptográficas a través de servicios de computación en la nube, la protección y seguridad de datos de la información crítica de las Pequeñas y Medianas Empresas (PYMES) y los desafíos que éstas enfrentan por falta de personal técnico especializado. Se destaca la importancia de aumentar la conciencia y educación en criptografía avanzada entre las PYMES, para fomentar su adopción segura de soluciones en la nube. Mediante el desarrollo de competencias internas y la colaboración con expertos en seguridad para una gestión de riesgos efectiva.

Palabras Claves: Criptografía, cifrado homomórfico, datos en la nube, PYMES, Seguridad.

Cloud cryptography: Impact on sme privacy through homomorphic encryption

ABSTRACT

Cryptographic systems in the cloud are studied in this review article. Focusing on homomorphic encryption and partially homomorphic cryptographic systems. Its applications, advantages, limitations and trends are analyzed; highlighting the ability of homomorphic encryption to process encrypted data, without the need to decrypt it and expose it to the cloud provider. The approach is aimed at the use of cryptographic technologies through cloud computing services, the protection and data security of critical information of SMEs and the challenges that they face due to lack of specialized technical personnel. Therefore, this article highlights the importance of increasing awareness and education in advanced cryptography among SMEs, to encourage their secure adoption of cloud solutions, through the development of internal competencies and collaboration with experts.

Keywords: Cryptography, homomorphic encryption; cloud data, SMEs, security.

==== o ====

Criptografia em nuvem: Impacto na privacidade de PMEs por meio da criptografia homomórfica

RESUMO

Sistemas criptográficos em nuvem são estudados neste artigo de revisão. Foco em criptografia homomórfica e criptosistemas parcialmente homomórficos. São analisadas suas aplicações, vantagens, limitações e tendências; destacando a capacidade da criptografia homomórfica de processar dados criptografados, sem a necessidade de descriptografá-los e expô-los ao provedor de nuvem. O foco está no uso de tecnologias criptográficas por meio de serviços de computação em nuvem, na proteção e segurança de informações críticas para Pequenas e Médias Empresas (PMEs) e nos desafios que elas enfrentam devido à falta de pessoal técnico especializado. A importância de aumentar a conscientização e a educação em criptografia avançada entre PMEs é destacada, para incentivar a adoção segura de soluções em nuvem. Por meio do desenvolvimento de competências internas e da colaboração com especialistas em segurança para uma gestão de riscos eficaz.

Palavras-chave: Criptografia, criptografia homomórfica, dados em nuvem, PMEs, Segurança.

==== o ====

INTRODUCCIÓN

La Computación en la Nube desempeña un papel fundamental en garantizar la seguridad y privacidad de los datos en las empresas, específicamente en la pequeña y mediana empresa (PYMES). Esto se debe a que, frente al aumento constante de amenazas como violaciones de información, accesos no autorizados y ataques cibernéticos, las PYMES se ven obligadas a recurrir a soluciones tecnológicas que les permitan proteger su información de manera efectiva. Sin embargo, el desconocimiento de las soluciones técnicas y de los proveedores del servicio provocan ciertos temores en la contratación de un entorno de computación en la nube (Rodríguez, 2020). Este temor, según diversos autores, es un obstáculo importante para la adopción plena de tecnologías en la nube por parte de las PYMES (Smith y Johnson, 2021).

Aunque la computación en la nube ofrece ventajas como la disminución de costos y el aumento de la eficiencia, las pequeñas y medianas empresas (PYMES) se enfrentan a importantes retos para garantizar la seguridad y privacidad de sus datos durante el proceso de migración a este entorno. No obstante, el desafío principal radica en desarrollar soluciones criptográficas que posibiliten a las PYMES beneficiarse de la computación en la nube mientras mantienen la seguridad y privacidad de su información intactas. La falta de soluciones criptográficas robustas y adaptadas a las necesidades de las PYMES puede llevar a la exposición de datos sensibles, lo que representa un riesgo significativo para su competitividad y reputación (Lee, 2019).

En cuanto a seguridad, una de las formas de proteger los activos de información en la "nube" es el uso de la criptografía. Este artículo analiza los sistemas criptográficos utilizados en cloud computing, describiendo los sistemas criptográficos homomórficos, el cifrado homomórfico de grupo, y sistemas parcialmente y completamente homomórficos. Estos métodos hacen posible que un servidor procese datos sin descifrarlos, siendo precisamente una de sus principales ventajas, ya que las empresas pueden cifrar sus bases de datos y subirlas a la "nube", sin posibilidad de que los datos queden expuestos al proveedor. La criptografía homomórfica, en particular, se presenta como una solución prometedora para abordar los desafíos de privacidad en la nube (Rivest et al., 1978).

Además, considerando que el servicio de cloud no es inmune a vulnerabilidades y fallos, se incluyen otros cifrados para la mejora de la privacidad. Finalmente se describe un aspecto importante sobre estos sistemas en las PYMES y su privacidad en la "nube". La idea principal es el uso de la criptografía para prevenir la violación de datos que, aunque sean hurtados, no puedan ser leídos. La implementación de medidas de seguridad adicionales, como la autenticación multifactor y la gestión de identidades, es crucial para complementar las soluciones criptográficas y garantizar una protección integral de los datos en la nube (Stallings, 2017).

Metodología

Este estudio se fundamenta en una revisión bibliográfica exhaustiva (Espinoza, 2020a), diseñada para explorar la intersección entre la criptografía en la computación en la nube y la protección de la privacidad de las PYMES a través del cifrado homomórfico. La metodología adoptada siguió un enfoque sistemático y riguroso, iniciando con la identificación y selección de fuentes relevantes en bases de datos académicas como IEEE Xplore, ACM Digital Library, ScienceDirect y Google Scholar, así como en buscadores especializados. Se emplearon términos clave como "criptografía en la nube", "cifrado homomórfico", "privacidad PYMES", y "seguridad de datos en la nube" para garantizar la amplitud y profundidad de la búsqueda (Brakerski y Vaikuntanathan, 2014).

El proceso de selección de información se caracterizó por su rigurosidad, priorizando artículos científicos revisados por pares, investigaciones financiadas por instituciones de prestigio como IARPA y DARPA, y documentación técnica especializada. Se aplicaron criterios de inclusión y exclusión basados en la relevancia, la calidad metodológica y la contribución al entendimiento de los objetivos del estudio. La extracción de datos se centró en identificar conceptos clave, metodologías de cifrado, casos de uso y análisis de impacto en la privacidad de las PYMES. Este análisis crítico de la literatura permitió sintetizar el estado del arte y fundamentar la discusión sobre cómo la criptografía, y en particular el cifrado homomórfico, puede fortalecer la seguridad y privacidad de los datos en la nube.

Adicionalmente, se consideraron los principios metodológicos de la investigación cualitativa, tal como lo sugieren Espinoza (2020b) y Espinoza y Toscano (2015), para garantizar una aproximación ética y sistemática en la revisión y análisis de la información. Este enfoque cualitativo permitió una comprensión profunda de las implicaciones teóricas y prácticas del

cifrado homomórfico en el contexto de la privacidad de las PYMES, asegurando que la interpretación de los datos fuera realizada con rigor y objetividad.

REVISIÓN DE LITERATURA

Fundamentos del Cifrado Homomórfico

El cifrado homomórfico constituye un progreso importante dentro del ámbito de la criptografía, ya que permite realizar operaciones directamente sobre datos encriptados sin requerir su desencriptación previa. Esto resulta especialmente valioso porque garantiza la privacidad de la información, incluso cuando se procesa en entornos externos como servicios en la nube. A continuación, se explicarán los fundamentos básicos del cifrado homomórfico y los distintos tipos existentes de métodos de cifrados empleados en la nube.

Analogía y funcionamiento básico del cifrado

En el contexto del cifrado, puede compararse con un sistema de casilleros o cajas de seguridad en un banco. Cada casillero tiene un número asignado que permite identificarlo fácilmente por su posición. El proceso de cifrado sería similar a tomar el contenido de uno de estos casilleros y moverlo a otro, siguiendo un patrón pseudoaleatorio que introduce un ruido intencional, dificultando saber dónde se encuentra el contenido original.

En este caso, la clave (*key*) funciona como una herramienta que indica cómo están organizados los casilleros y dónde se encuentra cada contenido, ya que no están distribuidos de manera uniforme ni de forma predecible. En el cifrado de clave pública, también llamado cifrado asimétrico, se hace uso de una clave para encriptar el mensaje y de otra distinta para desencriptarlo. En cambio, el cifrado de clave privada o simétrico utiliza una única clave que sirve tanto para encriptar como para desencriptar la información (Romero et al., 2017).

Cifrado Homomórfico

Este cifrado nace alrededor de los años 70, sin embargo, sus verdaderos cimientos se desarrollan en el año 2009, con la investigación iniciada por Craig Gentry, descrita en su tesis doctoral. Él propone realizar operaciones con datos cifrados sin tener que descifrarlos, de tal forma que se conoce la operación que se está efectuando, pero no los datos.

Este sistema fue desarrollado en IBM y se clasifica en cuatro escalas diferentes: una pequeña, denominada 2^9 con 512 dimensiones; otra de 2^{11}; una mediana de 2^{13}; y la más grande, de 2^{15}. Si bien resulta sencillo imaginar un cubo en tres dimensiones, puede parecer complicado visualizar una figura con 512 dimensiones; sin embargo, desde el punto de vista matemático, es completamente posible.

A manera de ejemplo, supóngase que se desea añadir dos valores: 2 y 3. Inmediatamente, estos valores se cifran convirtiéndose el 2 en 30 y el 3 en 38. Posteriormente, los datos cifrados se envían a la "nube" para procesar la información, devolviendo como resultado el valor 68. Por último, se descarga el valor y se descifra para obtener la respuesta final que es 5. En la **¡Error! No se encuentra el origen de la referencia.**, se presenta la idea principal del cifrado homomórfico (Naone, 2011).

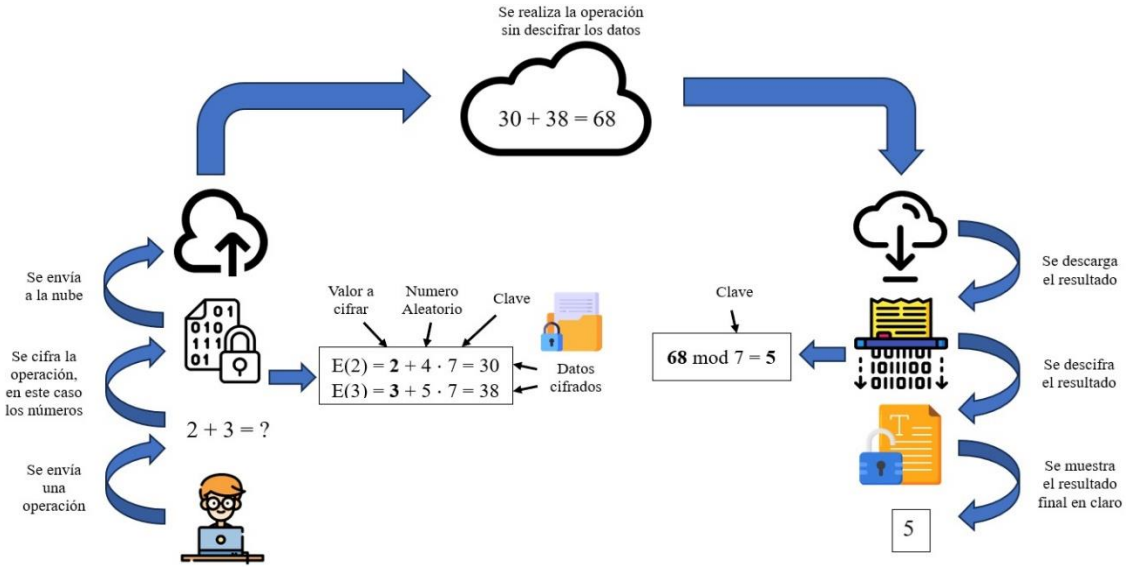

Figura 1. Cifrado Homomórfico.

La idea central consiste en que una empresa, independientemente de su magnitud, pueda cifrar su base de datos y subirla en algún servicio de "nube", sin la posibilidad de que en el proceso los datos queden expuestos al proveedor del servicio. De igual forma, brindar la misma seguridad al momento de descargar y descifrar la información, evitando que algún tercero tenga acceso a los datos no cifrados.

Por consiguiente, el sistema propuesto por Gentry fue capaz de procesar un limitado número de operaciones básicas utilizando datos cifrados, no obstante, no cumplía con las expectativas esperadas. En primera instancia, la solución fue la de emplear una capa de cifrado adicional para salvaguardar los resultados intermedios durante el colapso del sistema y el reinicio del mismo. No obstante, la doble capa de cifrado provocó que el sistema opere con extrema lentitud, lo cual no es apto para uso práctico.

Habitualmente las funciones de cifrado constan de una entrada de texto en plano X, y como salida se obtiene un texto cifrado Y. Además, incluyen dos operaciones como la adición y la multiplicación (+, □) en los textos planos y en los textos cifrados (⊕, ⊗) respectivamente. Se denomina funciones de cifrado homomórficos cuando se obtienen resultados iguales al procesar operaciones sobre X, así como en Y (Hemenway y Ostrovsky, 2012).

Cuando la función de cifrado (C) soporta las dos operaciones algebraicas, como son la adición y multiplicación, se denomina: sistemas criptográficos completamente homomórficos. Así mismo, los sistemas criptográficos parcialmente homomórficos o también llamados algo homomórficos, suelen soportar un número ilimitado de una operación, pero sólo un número limitado de la segunda operación. Por último, el sistema de cifrado que soporta solo una operación algebraica que puede ser homomorfismo aditivo o multiplicativo es denominado: sistemas homomórfico de grupo (Hrestak y Picek, 2014).

Entonces, el número de operaciones soportadas dependen de la elección del esquema de cifrado (Busatto, 2013). En la siguiente Tabla 1 se clasifican los esquemas criptográficos correspondientes a los tipos de cifrado:

Tabla 1.
Tipos de Cifrados Homomórficos

Tipo de cifrado	***Sistema criptográfico***	***Operaciones sobre los textos planos***	
		Suma	**Multiplicación**
Homomórfico de grupo	RSA, ElGamal	Ninguno	Sin límite
	Paillier, ElGamal (variante)	Sin límite	Ninguno
Parcialmente homomórfico	Paillier, ElGamal	Sin límite	Limitado (1 a BGN)
Completamente homomórfico	Gentry	Sin límite	Sin límite

Fuente: Rass et al. (2013).

En la práctica, el cifrado homomórfico brinda protección a los textos cifrados que se envían al proveedor de servicio de *cloud* que, sin el conocimiento de la clave secreta, no podrá ver ni mucho menos entender la información crítica de la empresa.

Cifrado homomórfico de grupo

Estos esquemas permiten calcular una operación en textos cifrados. El conjunto X representa a todos los mensajes posibles en texto claro, que el criptosistema utiliza como entrada para codificar bajo una clave pública *pk*. El conjunto Y representa a todos los textos cifrados. Las operaciones $\cdot$, $\otimes$ se definen como operaciones lógicas (Armknecht et al., 2010).

Entonces, para el cifrado C: $X \rightarrow Y$, de modo que $C(x) = y$, siendo que, $y \in Y$; y $x \in X$ (Agievich et al., 2015). Será un homomorfismo si satisface la siguiente condición: Dadas $(x1, x2) \in X$, dos mensajes cualesquiera:

- **Ecu 1:**

$$C(x1 \cdot x2; pk) = C(x1; pk) \otimes C(x2; pk) = y1 \otimes y2.$$

Donde:
$C(x1, pk) = y1 \rightarrow$ cifra x1 utilizando la clave pública pk para obtener texto cifrado y1

$C(x2, pk) = y2 \rightarrow$ cifra x2 utilizando la clave pública pk para obtener texto cifrado y2

Por consiguiente, para descifrar cualquier par de textos cifrados $y1 = C(x1; pk)$; y $y2=C(x2; pk)$, se debe emplear la clave secreta sk para descifrar D, entonces se tiene:

- **Ecu 2:**

$$D= (y1 \otimes y2; sk) = x1 \cdot x2$$

Donde:
$D= (y1 \otimes y2; sk) = x1 \cdot x2 \rightarrow$ descifra y1 y y2 utilizando la clave secreta sk para obtener texto plano x1 y x2.

La funcionalidad del presente cifrado, consiste en enviar la información cifrada al proveedor de servicio de "nube", donde se almacena en algunos casos, y en otros se realiza el cálculo solicitado sobre los datos cifrados. Finalmente, para descifrar el resultado, se usa la clave secreta que únicamente la conoce el destinatario. En la gráfica siguiente se ilustra en la **¡Error! No se encuentra el origen de la referencia.**, un escenario respecto a lo anterior.

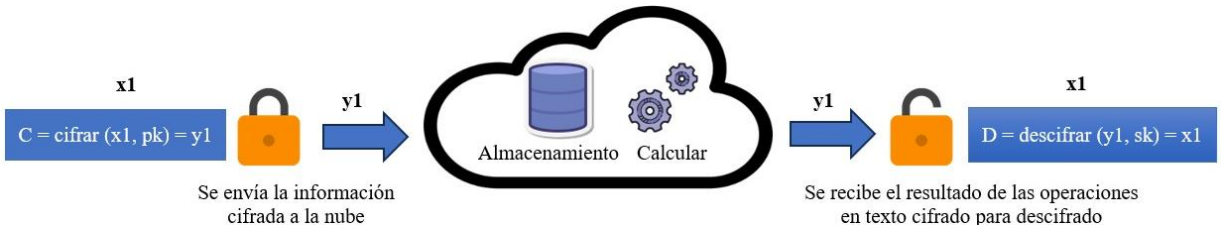

Figura 2. Escenario Cifrado Homomórfico de grupo.

Se conocen algunos esquemas de cifrado, cada uno con ciertas variaciones que proponen un aumento del nivel de seguridad en los datos. Entre los sistemas criptográficos que proporcionan un homomorfismo de grupo están: RSA, ElGamal y Paillier en sus primeras versiones.

Sistemas parcialmente homomórficos

En los últimos treinta años o más han existido varios sistemas de cifrado que pertenecen a la clase de sistemas de cifrado parcialmente homomórficos. Estos sistemas permiten aplicar muchas operaciones de un sólo tipo, mientras que de la otra operación únicamente se permite un número limitado de operaciones, por lo que son más sofisticados que los esquemas homomórficos de grupos. Un sistema parcialmente homomórfico demanda una cantidad considerable de dimensiones, al menos 512, para poder procesar anchos de palabra que alcanzan los 200.000 bits. (Alvarez et al., 2014).

Uno de los primeros esquemas destacados es el de Boneh-Goh-Nissim (BGN), que permitía realizar un número ilimitado de sumas, pero estaba limitado a una sola operación de multiplicación (Boné et al., 2005). Posteriormente, aparece el esquema SHE (por sus siglas en inglés *Somewhat Homomorphic Encryption*), conocido como cifrado algo homomórfico, debido a que posee algunas propiedades homomórficas que permiten evaluar circuitos correspondientes a funciones booleanas.

El cifrado SHE puede generar una cantidad definida de sumas y multiplicaciones; sin embargo, cada operación efectuada aporta ruido al texto cifrado, lo que provoca, al ser demasiado grande, que sea imposible descifrar el texto. Por último, en los esquemas SHE, la longitud del texto cifrado crece exponencialmente, lo que generan una gran longitud, causando que se violente el principio de los textos cifrados compactos (Silverberg, 2013).

Alves et al. (2014), describen los sistemas parcialmente homomórficos, entre los que sobresalen: los esquemas de Paillier y ElGamal.

Esquemas Paillier

En 1982 se propone el sistema criptográfico de Goldwasser-Micali, el mismo que se enfoca en la problemática de la factorización de enteros (Goldwasser y Micali, 1982), (Katz y Lindell, 2015). Su funcionamiento se describe a continuación:

- **Generación de claves:**
  1. Seleccionar 2 números primos *p*, *q* del mismo orden y calcular $(n) = p * q$
  2. Calcular $\phi(n) = (p-1) * (q-1)$

- **Cifrado**: Dado la clave pública *n* y un mensaje $m \in Z_n$
  1. Definir un número aleatorio $r \in Z_n^*$ y el mensaje *m.*
  2. Se obtiene como salida el mensaje cifrado: $c= [(1 + n)^m * r^n \bmod n^2]$

- **Descifrado**: Dado la llave privada (ϕ(n)) y el texto cifrado c. A la salida se obtiene el texto en claro *m*:
  1. Calcular $m = (\frac{[(c^{\phi(n)} \ mod \ n^2)] - 1}{n} * \phi(n)^{-1} \ mod \ n)$

El consumo de recursos computacionales para ejecutar el cifrado en el esquema Paillier, dependerá básicamente de una exponenciación y una multiplicación del módulo n2. Por otro lado, la seguridad proporcionada por este esquema resulta insuficiente; por esta razón, es fundamental complementarlo con una función de firma digital para proteger adecuadamente los datos.

Esquema ElGamal

En 1985, Taher ElGamal propone el esquema ElGamal, el mismo que ha sufrido diversas variaciones en la función de cifrado y firma digital. Su funcionamiento se describe a continuación:

- **Generación de claves:**
  1. Seleccionar un primo *p* grande y
  2. Seleccionar 2 número aleatorios: un elemento generado *g* del grupo cíclico (Z_p^*) y *a* que funcionará como clave privada.
  3. Calcular $\beta = g^a \ mod \ p$
  4. Entonces (*p*, *g*, *β*) como la clave pública y (*a*) como clave secreta.

- **Cifrado**: Dado la clave pública *(p, g, β)* y un mensaje *m*,
  1. Seleccionar aleatoriamente $b \in \{Z_{p-1}^* - \{1\}\}$
  2. Calcular $Y1 = g^b \ mod \ p$
  3. Calcular $Y2 = \beta^b m \ mod \ p$
  4. El texto cifrado corresponde a: C_b (m, b) = (y_1, y_2)

- **Descifrado**: Dado la clave privada *(a)* y un texto cifrado *c:*
  1. Con teorema de Fermat calcular

- **Ecu 3:**

$$m = y_1^{p-1-a} \ y_2 \ mod \ p$$

Por lo tanto, según la revisión bibliográfica realizada, se alega que los sistemas parcialmente homomórficos, permiten realizar cálculos limitados sobre los datos cifrados, sin embargo, ciertos esquemas propuestos recientemente, como es el caso del esquema BGV, permiten evaluar circuitos algebraicos de profundidad multiplicativa L en tiempo O(λL3) (Brakerski et al., 2014). Estas mejoras en el esquema precitado, contribuyen directamente en hacer efectiva la encriptación completamente homomórfica o también conocida como ECH, con la finalidad de resolver problemas prácticos (Naehrig et al., 2011).

Existe una libertad en la elección de parámetros del esquema BGV, de modo que se sugieren diversas opciones de parámetros para diferentes escenarios, dependiendo de la posibilidad de uso de operaciones en bloque, de la cantidad de multiplicaciones involucradas y de la profundidad del circuito. Por ejemplo, una propuesta práctica es el sistema CryptDB, que es una base de datos sobre datos cifrados (Popa et al., 2011). Se utilizan varios empalmes criptográficos para permitir consultas SQL arbitrarias. Las operaciones se agrupan así: 1) verificación de igualdad; 2) comparación de orden; 3) operaciones

aritméticas; y 4) uniones. Se emplean varias capas anidadas de cifrado para resolver cada uno de estos grupos.

Aunque, el sistema ofrece un nivel de confidencialidad robusto, la seguridad no es garantizada. Sin embargo, la idea prácticamente es interesante, porque a más de ser eficiente es transparente para el usuario, debido a que el servidor de bases de datos interpreta las consultas SQL de forma dinámica empleando funciones internas del motor de la base. Por tal motivo, se consigue brindar resguardo de los datos en contra del administrador de la base de datos (Morais y Dahab, 2012).

El cifrado parcialmente homomórfico es aplicado a varios contextos, es así que en algunos países donde se ha empleado un sistema de voto electrónico, como Votebox y Helios, se ha utilizado el esquema ElGamal para efectuar el conteo de los votos cifrados y garantizar la confidencialidad (Cabarcas, 2015). En este escenario únicamente se necesita sumar 1 a una cantidad de votos y no es necesario multiplicar cantidades.

Sistemas completamente homomórficos

Los sistemas de cifrado completamente homomórficos o también conocido como FHE (por sus siglas en inglés *Fully Homomorphic Encryption*), soportan las dos operaciones, adición y multiplicación directamente sobre datos cifrados, por lo que son la clase más sofisticada dentro de los métodos de cifrado homomórfico. El tamaño de la clave pública en este sistema es de 17MB y necesita exactamente 2.4 segundos para generarse; mientras que en un sistema con 32768 dimensiones (2^{15}) se requiere aproximadamente 2 horas y ocupa 2.3GB (Alvarez et al., 2014).

El primer esquema totalmente homomórfico fue propuesto por Craig Gentry, el mismo que inició de un esquema parcialmente homomórfico que, como se analizó anteriormente, fue capaz de ejecutar un número finito de operaciones sobre el texto cifrado (Gentry, 2009). Además, el esquema de Gentry fue un referente, de modo que permitió la construcción de otros esquemas cifrados homomórficos, como es el caso del esquema DGHV (Bilar, 2015).

En los esquemas completamente homomórficos se fundamentan tres principales problemas matemáticos: a) reticulados ideales, propuesto por Gentry y Gentry-Halevi; b) anillos de números enteros, propuesto por Dijk, Gentry, Halevi y Vakuntanathan, empleado por el esquema DGHV; c) problema de aprendizaje de máquina LWE, propuesto por Brakerski y Vaikuntanathan (Bilar et al., 2015).

Rass, Stefan y Slamanig (2013), afirman que un sistema completamente homomórfico está compuesto de los siguientes algoritmos:

- **Algoritmo para generar claves:** Utiliza un parámetro de seguridad y genera 3 claves: 1) clave pública *pk*; 2) clave de evaluación pública *evk*; y 3) clave secreta *sk*.
- **Algoritmo de cifrado:** Toma un mensaje m, la clave pk y envía un cifrado.

Ecu 4:

$$c = \text{cifrado}(m; pk). \in \{0, 1\}$$

- **Algoritmo de descifrado público:** Algoritmo determinista que toma un cifrado c y una clave secreta sk y salidas.

Ecu 5:

$$m = \text{descifrado}(c; sk)$$

- **Algoritmo de evaluación:** Toma una clave de evaluación evk, una función f:{0, 1}k -> {0, 1}, k cifrados y genera un texto cifrado

Ecu 6:

$$cf = eval\ (f, c1,..., ck; evk)$$

En un contexto de un cifrado completamente homomórfico, los mensajes se definen como bits, provocando que los espacios de mensajes sean más grandes. Lo que realmente importa es que las funciones relacionadas con el parámetro de seguridad, proporcionen el mismo resultado al descifrar el texto cifrado como si evaluaría *f* en el texto claro. Por lo tanto, es necesario que los esquemas FHE sean compactos, esto significa que la longitud de salida del algoritmo de evaluación esté restringida a un polinomio en el parámetro de seguridad, tomando en cuenta que esto no depende del número de entradas de *f* ni de la función *f* misma (Rass et al., 2013).

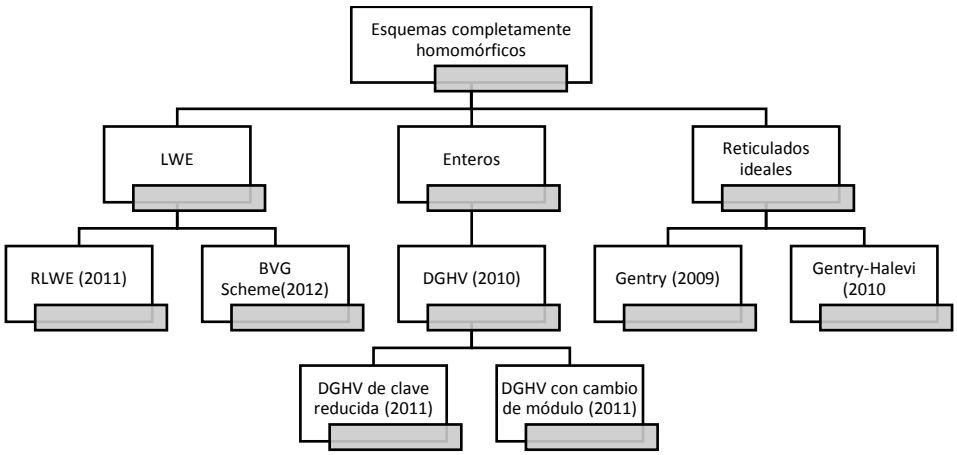

Figura 3. Clasificación de los esquemas completamente homomórficos
Fuente: Elaborado a partir de Bilar et al. (2015).

Esquemas totalmente homomórficos basados en reticulados

Como ya se ha mencionado, Gentry propuso el primer esquema totalmente homomórfico, conocido por su doble capa de cifrado, proceso que inicialmente se llamó Recrypt. No obstante, propuso un procedimiento llamado bootstraping, que reducía el ruido generado por el doble cifrado, permitiendo dar a un esquema originalmente SHE las características de ser totalmente homomórfico. Este esquema creado por Gentry, utiliza como base reticulados ideales y su implementación fue sobresaliente, siendo reconocido como un gran avance en esta área (Ogburna et al., 2013).

Posteriormente, Halevi empleo el esquema de arranque de Gentry y juntos en el 2010 propusieron el esquema totalmente homomórfico Gentry-Halevi, el mismo que se caracteriza por la optimización en la generación de claves.

Esquemas totalmente homomórficos basados en números enteros

En el 2010 Dijk, Gentry, Halevi y Vaikuntanathan presentaron el esquema DGHV (nombrado así por las iniciales de los cuatro autores), que se caracteriza por utilizar únicamente álgebra modular sobre un anillo de números enteros, siendo matemáticamente algo menos complejo en comparación con los esquemas basados en reticulados. Luego este esquema fue analizado por Coron, el mismo que realizó dos variantes para reducir el costo

computacional y reducir el tamaño de la clave pública, mediante técnicas de reducción y comprensión.

La primera variante de Coron, llamada DGHV con llave reducida, consta de la suma de otros parámetros cuadráticos agregados al esquema para almacenar un conjunto pequeño de valores vinculados a la clave pública, para posteriormente, en tiempo de ejecución, generar la clave pública completa de una orden de $\mathcal{O}$ (λ10) a $\mathcal{O}$ (λ7) (Coron et al., 2012).

En la segunda variante, conocida como DGHV con compresión de claves y cambio de módulo, los elementos de la clave se generan mediante un generador de números aleatorios (RNG, por sus siglas en inglés, *Random Number Generator*), lo que permite recuperar los parámetros de la clave durante la ejecución. Además, Coron redujo aún más el tamaño de la clave pública generada por el esquema, siendo de un orden de $\mathcal{O}$ (λ7) a $\mathcal{O}$ (λ5) (Coron et al., 2012).

Esquemas totalmente homomórficos basados en LWE

Esquema desarrollado por Brakerski y Vaikuntanathan (2014), quienes desarrollaron dos técnicas: una de reducción de tamaño y la otra de cambio de módulo. Con estas nuevas técnicas el ruido en el texto cifrado crece de forma casi lineal, y la técnica de *bootstraping*, considerada ahora la parte no importante del sistema, queda desplazada por la optimización del rendimiento del esquema.

Las PYMES y la privacidad en la "nube"

La constante evolución de Internet ha permitido replantear los conceptos de computación desde una nueva perspectiva. En la actualidad, la computación en la nube, también conocida como *cloud computing*, ofrece acceso a un conjunto amplio y configurable de recursos computacionales que pueden ser gestionados y compartidos a través de técnicas de virtualización, con un mínimo esfuerzo administrativo y, lo más importante, a un costo reducido. Pero aún en este escenario favorable existen problemas relacionados principalmente con: la seguridad, la privacidad en el recurso compartido y la falta de confianza en el proveedor.

Sobre la base de lo examinado anteriormente, se puede asegurar que los problemas de privacidad pueden ser solucionados con el uso del cifrado homomórfico, el cual permite manipular los datos sin necesidad de descifrarlos. Además, existen varias aplicaciones que requieren sólo un número limitado de operaciones, que bastaría con utilizar el sistema de cifrado parcialmente homomórfico, siendo lo más óptimo (Hrestak y Picek, 2014).

En la actualidad, se han llevado a cabo numerosas investigaciones con el objetivo de mejorar los esquemas homomórficos y asegurar la protección de los datos en entornos de computación en la nube. Un ejemplo de ello son los trabajos descritos por Ramírez y Mora (2014):

- IARPA, del inglés *Intelligence Advanced Research Projects Activity*, que ha financiado la investigación sobre seguridad y aseguramiento de la privacidad, tiene como objetivo garantizar el intercambio de datos seguros de ambas partes, empleando un cifrado completamente homomórfico. Estas técnicas se aplicarán en diversos contextos, tales como el almacenamiento externo, donde se busca garantizar la integridad y confidencialidad de los datos almacenados; la consulta de bases de datos, permitiendo realizar búsquedas seguras sin comprometer la privacidad de la información; los sistemas de publicación y suscripción, que facilitan la distribución de contenido de manera eficiente y protegida; así como en los servicios de correo electrónico, asegurando la seguridad en la comunicación y el intercambio de mensajes. Además, estas aplicaciones son fundamentales en entornos donde la

protección de datos sensibles es una prioridad, como en el ámbito empresarial y gubernamental.

- DARPA o Defense Adva*nced Research Projects Agency*, financió el proyecto Cálculo de programación en datos cifrados, que tiene como finalidad buscar nuevos y mejorados mecanismos que permitan manipular datos cifrados de una manera más eficiente.

En el año 2013, IBM presenta la biblioteca *Helib* para el FHE. Esta biblioteca de software de código abierto, posee implementaciones del esquema Brakerski-Gentry-Vaikuntanathan, junto con muchas optimizaciones para hacer la evaluación homomórfica más rápida. "HElib está escrito en C++ y utiliza la biblioteca matemática NTL, sin embargo, no tiene la aplicación de bootstrapping, pero fue agregado en diciembre de 2014. En marzo de 2015, HElib también soporta multi-procesos" (Halevi y Shoup, 2014).

Por lo tanto, el uso de la criptografía homomórfica o cifrado homomórfico es la solución para el problema de privacidad en la "nube". Sobre la base del ligero análisis presentado, es evidente que seguirán surgiendo muchos más mecanismos que acelerarán y mejorarán los procesos con textos cifrados. Pero también, es importante tener en cuenta que la desconfianza, las dudas y los cuestionamientos de las PYMES, en migrar sus bases de datos a un proveedor de *cloud*, es poco razonable. Aun así, la tendencia sobre el uso de cloud está ganando terreno paulatinamente, por lo que se puede asegurar que las PYMES empezarán a interesarse de a poco por este tema (Coron et al., 2011).

En efecto, independientemente del tamaño de la organización, los factores clave para garantizar su funcionamiento eficiente, siempre serán la necesidad por los sistemas de información, procesamiento, bases de datos y óptimos niveles de seguridad y privacidad, que se pueden ser encontrados utilizando el poder computacional de la "nube" (Hrestak y Picek, 2014).

Justamente un ambiente cloud proporciona muchos beneficios para las PYMES, de entre los que se pueden mencionar: optimizar la oferta de servicios, aumentar la competitividad y adaptar la estrategia del negocio a los requerimientos del mercado.

Además, el ahorro económico es otro factor que beneficia a las PYMES, puesto que al migrar a un entorno virtualizado no requiere un centro de datos local. Por otro lado, la confiabilidad en las operaciones garantizará la permanente disponibilidad y accesibilidad a los datos, descartando cualquier interrupción en el sistema. Por último, la eficiencia en los procesos permite la automatización de las tareas internas reduciendo los tiempos de ejecución de las mismas. Consecuentemente, el tipo de negocio no es un impedimento para acceder a tales beneficios, más bien el potencial que ofrece la computación en la "nube", permite catapultar el modelo de negocio de este tipo de empresas con las seguridades criptográficas necesarias.

En efecto, los escenarios prácticos donde podrán ser utilizados los sistemas de cifrado homomórfico son innumerables, por lo que se espera en un futuro no tan lejano acceder al poder computacional que ofrece *cloud*, junto con sistemas de cifrado homomórficos más eficientes, para la seguridad y confidencialidad de los datos.

Para las PYMES, es una gran opción optar por una arquitectura virtualizada, por lo que el éxito de lograr una ventaja competitiva dependerá del proveedor de *cloud*, del modelo de servicio a contratar y de la adaptación a los nuevos ambientes tecnológicos. Los beneficios se reflejarán en la reducción de costos, incremento de la seguridad, permanente disponibilidad, fácil operatividad y sobre todo confiabilidad en las transacciones.

Riesgos en la implementación

El análisis de los riesgos asociados a la implementación de los servicios *cloud* en las PYMES, revela varias preocupaciones. En la investigación realizada por Guevara y Soriano (Guevara & Soriano, 2022), a varias PYMES del país, señalan que el principal riesgo es la insuficiencia de habilidades internas, identificada por el 45% de las empresas encuestadas, seguida por el 32%, debido al miedo a problemas de seguridad en el almacenamiento. Otros riesgos incluyen temores sobre la legalidad de los datos, brechas de seguridad y rendimiento insatisfactorio, cada uno con aproximadamente un 20% de riesgo. Las normativas internacionales y la dependencia de proveedores fueron los menos mencionados, con un 18% y 11% respectivamente. Estos hallazgos sugieren que la resistencia a adoptar la nube podría deberse principalmente a la falta de conocimientos técnicos internos (Agievich et al., 2015).

Tendencias actuales

El cifrado homomórfico ha incrementado en gran medida sus aplicaciones y métodos para un procesamiento veloz y eficiente. No obstante, a través del tiempo se observan los avances realizados. Por ejemplo, investigaciones como el de Salman et al. (2021), indican que el cifrado homomórfico se considera como solución sofisticada y potente al sistema de criptografía, preservando datos sin exposición al proveedor. Sin embargo, el cifrado homomórfico tiene gastos generales como claves de gran tamaño y textos cifrados largos; y como resultado un largo tiempo de ejecución. Como solución, establecen un análisis de big data basada en clustering y la Criptografía de curva elíptica (ECC). Donde, la técnica de agrupamiento (EDC) divide *big data* en varios subconjuntos de nodos de computación en la nube. El uso de técnicas híbridas mejora el rendimiento y la eficiencia del análisis de *bigdata* y al mismo tiempo mantienen los datos protegidos.

Por su parte el estudio de Priya y Karthick (2022), determinó en su investigación que, el algoritmo de marco liviano es significativamente más rápido que el algoritmo existente, casi 1,2 veces más rápido que el algoritmo de criptografía de curva elíptica. El algoritmo planteado es más rápido en la recuperación de datos, el cifrado y eliminación de datos redundantes en comparación con el método existente.

Por otro lado, Al-Odat et al. (2020), presenta una criptografía Hash, para aplicaciones de *BigData* y la *IoT*. En este diseño, emplean S-Box, transformación lineal y las funcionalidades de la permutación de bits. Con esto logran, resultados de velocidad, memoria y consumo de energía. Murali y Prasad (2017), realizan un análisis comparativo de varias técnicas criptográficas de criptografía cuántica. Kumar (2021) menciona que la computación en la nube ha cambiado de forma radical, que su uso va más allá que sólo utilitario, llevando a la manipulación de datos. No obstante, realiza una comparación entre los diversos tipos de encriptación que existen y su vulnerabilidad.

Resaltando que el algoritmo AES utiliza una estructura algebraica considerada demasiado simplista, con niveles de seguridad relativamente bajos, ya que cada bloque emplea el mismo esquema de cifrado, lo que lo hace vulnerable a ataques de tipo MITM (Man-In-The-Middle). Por ello, resulta fundamental incrementar los niveles de protección en dichos esquemas. En este contexto, la investigación resalta el uso de la criptografía basada en ADN, la cual permite cifrar grandes volúmenes de datos con un procesamiento mínimo gracias a las propiedades únicas del ADN.

Por consiguiente, para mejorar el método de encriptación, combina ambas metodologías tanto la ADN como AES. Este método es esencial para sistemas que requieren más de una capa de seguridad, dando a conocer que, en un futuro cercano, será esta tecnología la que permite combinación como la transferencia de secuencias de ADN, convirtiendo la misma en una de las mayor robustez y rango de seguridad. Así también, Acharya et al. (2021),

describe una propuesta mejorada de Criptografía de Curva Elíptica (ECC por sus siglas en ingles *Elliptic Curve Cryptography*), para el aseguramiento de los datos. Hong (2016), indica que la computación en la nube, se ha convertido hoy en día, el principal modelo en el futuro debido a ventajas como alto recurso, tasa de utilización y ahorro con alto rendimiento.

Entre los diversos métodos disponibles, se incluyen la Seguridad de Computación Multipartita (SMC, por sus siglas en inglés Sec*ure Multi-Party Computation*) y el uso de un Tercero de Confianza (TTP, por sus siglas en inglés *Trusted Third Party*).No obstante, los autores en esta investigación proponen la curva elíptica con esquema de cifrado homomórfico basado en criptografía (ECC), orientado con SMC, para reducir con ello, drásticamente el cálculo de costo de comunicación. Como evidencia, se aplica este método al cifrado basado en ECC al cálculo de datos GPS en terremoto, probando que el esquema es confiable y mantiene un excelente efecto de cifrado con alta seguridad.

Por su parte Guesmi y Saidane (2017), y Suryawanshi y Shelke (2016), analizan los sistemas de encriptación como con métodos para mejoramiento de la confiabilidad y el uso del mismo en auditorías públicas. Además, Shukla (2022), determina que, la computación en la nube ayuda en numerosos caminos para las redes de servicios basadas en la web. Esto incluye la salvaguardia de los datos sensibles con mayor precisión, acompañado de inteligencia con algoritmo criptográfico para la obtención de datos seguros en la nube del sistema. Se logra con un sistema de gestión de almacenamiento que incorpora *big data* utilizando algoritmo de criptografía. Finalmente, Yang y Yu (2014), realiza el estudio de la seguridad de datos en el ciberespacio usando el método de criptografía. Mientras que Saroj et al (2015), analiza la seguridad de datos en criptografía de umbral en computación en la nube.

Por lo que, en esta sección hemos analizado algunas de las tantas aplicaciones para la encriptación de datos para pequeñas, medianas o grandes empresas que involucren cantidades diversas de datos.

LIMITACIONES DEL ESTUDIO

Este estudio de revisión se limita a la exploración de la literatura académica y técnica disponible hasta la fecha sobre el cifrado homomórfico y su impacto en la privacidad de las pymes en entornos de nube. La naturaleza emergente de esta tecnología implica que algunas implementaciones prácticas y casos de uso específicos pueden no estar completamente documentados o ser de acceso restringido. Además, la rápida evolución de los estándares de seguridad y las regulaciones de protección de datos podrían requerir actualizaciones futuras de este análisis.

ESTUDIOS FUTUROS

Se recomienda que futuras investigaciones se centren en el desarrollo de marcos de implementación de cifrado homomórfico adaptados a las necesidades específicas de las pymes, considerando factores como el costo, la facilidad de uso y el rendimiento. Asimismo, es crucial explorar la integración de esta tecnología con otras soluciones de privacidad y seguridad en la nube, como la computación multipartita segura y la privacidad diferencial. También sería valioso realizar estudios de caso detallados sobre la adopción de cifrado homomórfico en diferentes sectores y contextos empresariales.

RECONOCIMIENTO

Los autores desean expresar su sincero agradecimiento a los docentes de la Universidad Técnica de Machala y a los docentes del Instituto Superior Tecnológico Ismael Pérez Pazmiño, por la valiosa colaboración y el apoyo brindado durante la realización de este

estudio. Su experiencia y conocimientos fueron fundamentales para la elaboración de este artículo de revisión.

CONTRIBUCIÓN DE LOS COAUTORES

Ángel Mauricio Ramón-Noblecilla:

- Como coordinador de la investigación, lideró la planificación y ejecución del estudio, asegurando la coherencia y el cumplimiento de los objetivos.
- Su experiencia en la gestión de proyectos de investigación fue fundamental para la organización y clasificación de la información recopilada.
- Realizó una revisión exhaustiva del borrador del manuscrito, garantizando la precisión y claridad del contenido, así como el estricto cumplimiento de las normas APA en las citas y referencias.
- Su capacidad para la organización y la revisión fue fundamental para la correcta culminación del proyecto.

Yasser Cesar Alvarado-Salinas:

- Se responsabilizó de la búsqueda y selección de información relevante en diversas bases de datos académicas, utilizando palabras clave estratégicas.
- Su capacidad de síntesis permitió la elaboración de resúmenes concisos y precisos de la literatura revisada.
- Fue el responsable de la redacción de la introducción del manuscrito, estableciendo el contexto y la relevancia del estudio de manera clara y convincente.
- Su capacidad de búsqueda y de redacción permitieron una buena recopilación de datos y una buena introducción.

Johnny Paul Novillo-Vicuña:

- Desempeñó un papel crucial en la elaboración de las síntesis detalladas de la información recopilada, facilitando la comprensión de los conceptos clave.
- Fue el autor principal del borrador inicial del manuscrito, demostrando su capacidad para integrar y organizar la información de manera coherente.
- Tras la retroalimentación de los coautores, se encargó de la revisión y depuración del manuscrito, asegurando la calidad y la cohesión del trabajo final.
- Su capacidad de síntesis y de redacción fueron cruciales para la elaboración del cuerpo del documento.

CONCLUSIONES

La Computación en la nube se ha consolidado como una herramienta esencial para las PYMES, ofreciendo soluciones avanzadas que permiten optimizar la gestión de datos y fortalecer la seguridad de la información. A través de sistemas de protección robustos, como el cifrado homomórfico, la recuperación ante desastres, el control de acceso y la colaboración segura, las PYMES pueden mitigar riesgos asociados a las amenazas cibernéticas y garantizar la privacidad de su información en un entorno digital cada vez más complejo y vulnerable.

Además, la adopción de tecnologías en la nube no solo mejora la seguridad, sino que también proporciona una ventaja competitiva significativa al permitir a las empresas acceder a recursos tecnológicos de última generación sin la necesidad de realizar grandes inversiones en infraestructura física. Esto resulta especialmente beneficioso para las PYMES, puesto que permite escalar sus operaciones de manera flexible, adaptándose a las demandas del mercado y optimizando sus procesos internos.

Así mismo el uso de criptografía avanzada, particularmente el cifrado homomórfico, permite abordar de manera eficaz los riesgos de privacidad en la computación en la nube. Además, se evidencia que, aunque existen desafíos en términos de la complejidad computacional y la eficiencia de los sistemas de cifrado homomórfico, los avances recientes y las inversiones en investigación y desarrollo están mejorando significativamente su viabilidad para aplicaciones prácticas. Esto sugiere un futuro prometedor donde las PYMES pueden aprovechar plenamente los beneficios de la nube sin sacrificar la seguridad de sus datos.

Finalmente, el estudio destaca la importancia de fomentar una mayor sensibilización y formación entre las PYMES acerca de las diversas opciones de seguridad existentes para garantizar la protección de los datos almacenados en la nube. A pesar de los riesgos potenciales, la resistencia a adoptar soluciones en la nube a menudo se basa en la falta de conocimiento sobre tecnologías criptográficas avanzadas como el cifrado homomórfico. Por lo tanto, es crucial fomentar una mejor comprensión de estas tecnologías y sus beneficios, así como promover el desarrollo de habilidades internas, para que las PYMES puedan tomar decisiones informadas sobre la seguridad de la información en entornos de computación en la nube.

REFERENCIAS

Acharya, S., Manoj, K., & Gayana, M. N. (2021). "Enhanced Performance and Data Security using Elliptic Curve Cryptography in Cloud Environment," in 2021 International Conference on Computational Performance Evaluation (ComPE). *IEEE*, 869–873. https://doi.org/10.1109/ComPE53109.2021.9751865

Agievich, S., Gorodilova, A., Kolomeec, N., Nikova, S., Preneel, B., Rijmen, V., . . . Vitkup, V. (2015). Problems, Solutions and Experience of the First International Student's Olympiad in Cryptography. *Applied Discrete Mathematics*, 1-23.

Al-Odat, Z. A., Al-Qtiemat, E. M., & Khan, S. U. (2020). "An Efficient Lightweight Cryptography Hash Function for Big Data and IoT Applications," in 2020 IEEE Cloud Summit. *IEEE*, 66-71. https://doi.org/10.1109/IEEECloudSummit48914.2020.00016

Alvarez, R., Santonja, J., & Zamora, A. (2014). Hacia la seguridad criptográfica en sistemas DaaS. *RECSI*, 297-240.

Alves, M. R., Criptográficos, M. A., & López, J. (2014). *Aplicação Conceitual de Criptografia Homomórfica.*

Armknecht, F., Katzenbeisser, S., & Peter, A. (2010). Group Homomorphic Encryption Characterizations, Impossibility Results, and Applications. *Designs, codes and cryptography*, 1-24.

Bilar, G. R. (2015). Classificação, implementação e desempenho de esquemas totalmente homomórficos sobre números inteiros e suas melhorias. *JADI*, 7-12.

Bilar, G. R., Dos Santos, L. C., & Pereira, F. D. (2015). Classificação, implementação e desempenho de esquemas totalmente homomórficos sobre números inteiros e suas melhorias. *Researchgate*.

Boné, D., Goh, E.-J., & Nissim, K. (2005). Evaluating 2-DNF formulas on ciphertexts. *In Theory of Cryptography Conference*, 325-341.

Brakerski, Z., & Vaikuntanathan, V. (2014). Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, 831-871.

Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 13.

Busatto, N. J. (2013). *Criptografia Homomórfica .* Brasília,.

Cabarcas, D. J. (2015). El voto electrónico y retos criptográficos relacionados. *Revista Facultad de Ciencias Universidad Nacional de Colombia*, 83-102.

Coron, J. S., Naccache, D., & Tibouchi, M. (2012). Public key compression and modulus switching for fully homomorphic encryption over the integers. *Springer*, 446-464.

Coron, J., Mandal, A., Naccache, D., & Tibouchi, M. (2011). Fully Homomorphic Encryption over the Integers with Shorter Public Keys. *Springer,*, 487-504.

Espinoza Freire, E. E. (2020a). La búsqueda de información científica en las bases de datos académicas. *Revista Metropolitana de Ciencias Aplicadas*, *3*(1), 31-35.

Espinoza Freire, E. E. (2020b). El problema, el objetivo, la hipótesis y las variables de la investigación. *Portal de la Ciencia*, *1*(2), 1-71.

Espinoza Freire, E. E., & Toscano Ruíz, D. F. (2015). *Metodología de investigación educativa y técnica*. Machala: UTMach. Recuperado de http://repositorio.utmachala.edu.ec/handle/48000/6704.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *STOC*, (págs. 169-178).

Goldwasser, S., & Micali, S. (1982). Probabilistic encryption & how to play mental poker keeping secret all partial information. *Proceedings of the fourteenth annual ACM symposium on Theory of computing. ACM*, 365-377.

Guesmi, H., & Saidane, L. A. (2017). "Improved Data Storage Confidentiality in Cloud Computing Using Identity-Based Cryptography," in 2017 25th International Conference on Systems Engineering (ICSEng). *IEEE*, 324-330. https://doi.org/10.1109/ICSEng.2017.32

Guevara, A. V., & Soriano, S. D. (2022). La nube en Pymes mediante las normas ISO 27005. *Ingeniería y sus Alcances, Revista de Investigación, 6*(15), 169-182. https://doi.org/https://doi.org/10.33996/revistaingenieria.v6i15.98

Halevi, S., & Shoup, V. (2014). Algorithms in HElib. *CRYPTO 2014: Advances in Cryptology* (págs. 554-571). Berlín, Heidelberg: Springer.

Hemenway, B., & Ostrovsky, R. (2012). On Homomorphic Encryption and Chosen-Ciphertext Security. *In International Workshop on Public Key Cryptography*, 52-56.

Hong, M.-Q., Wang, P.-Y., & Zhao, W.-B. (2016). "Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance an. *IEEE*, 152-157. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.51

Hrestak, D., & Picek, S. (2014). Homomorphic Encryption in the Cloud. *Electronics and Microelectronics (MIPRO), 2014 37th International Convention* , 1400-1404.

Hrestak, D., & Picek, S. (2014). Homomorphic Encryption in the Cloud. *Information and Communication Technology, Electronics and Microelectronics* , 1400-1404.

Kabir, N., & Kamal, S. (2020). "Secure Mobile Sensor Data Transfer using Asymmetric Cryptography Algorithms," in 2020 International Conference on Cyber Warfare and Security (ICCWS). *IEEE*, 1-6. https://doi.org/10.1109/ICCWS48432.2020.9292392

Katz, J., & Lindell, Y. (2015). *Introduction to Modern Cryptography, Second Edition.* Boca Raton: Taylor & Francis Group .

Kumar, A. (2021). "Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing," in 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). *IEEE*, 1529–1535. https://doi.org/10.1109/I-SMAC52330.2021.9640708

Morais, E., & Dahab, R. (2012). Encriptação homomórfica. *Minicursos do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 151-195.

Murali, G., & Prasad, R. S. (2017). "Comparison of cryptographic algorithms in cloud and local environment using quantum cryptography," in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). *IEEE*, 3749–3752. https://doi.org/ 10.1109/ICECDS.2017.8390165

Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). Can homomorphic encryption be practical? *In Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM*, 113-124.

Naone, E. (19 de Abril de 2011). *MIT technology review*. http://www2.technologyreview.com/news/423683/homomorphic-encryption/

Lee, H. (2019). *Cloud Security for Small and Medium Enterprises*. Journal of Information Security, 10(2), 45-62.

Ogburna, M., Turnerb, C., & Dahalc, P. (2013). Homomorphic Encryption. *ScienceDirect*, 502-509.

Popa, R. A., Redfield, C., Zeldovich, N., & Balakrishnan, H. (2011). Cryptdb: protecting confidentiality with encrypted query. *In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, 85-100.

Priya, K. T., & Karthick, V. (2022). "A Non Redundant Cost Effective Platform and Data Security in Cloud Computing using Improved Standalone Framework over Elliptic Curve Cryptography Algorithm," in 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS. *IEEE*, 1249-1253. https://doi.org/10.1109/ICSCDS53736.2022.9761002

Ramírez, D. E., & Mora, H. M. (2014). Criptografía en Bases de datos en Cloud Computing. *AiBi. Revista de investigación en administración e ingeniería*, 39-48.

Rass, Stefan, & Slamanig, D. (2013). *Cryptography for Security and Privacy in Cloud Computing.* Norwood,: Artech House.

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. In *Foundations of secure computation* (pp. 169-180). Academic Press.

Rodríguez, G. S. (2020). Privacidad y seguridad en la nube: algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo. *LEX, 18*(1), 229-358. https://doi.org/http://dx.doi.org/10.21503/lex.v18i25.2109

Romero, C., Alvarado, Y., & Paladines, N. (2017). Criptografía y Seguridad en m-commerce. *Ciencia y Tecnología*, 144-177.

Salman, Z., Hammad, M., & Al-Omary, A. Y. (2021). "A Homomorphic Cloud Framework for Big Data Analytics Based on Elliptic Curve Cryptography," in 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). *IEEE*, 7-11. https://doi.org/10.1109/3ICT53449.2021.9582001

Saroj, S. K., Chauhan, S. K., Sharma, A. K., & Vats, S. (2015). "Threshold Cryptography Based Data Security in Cloud Computing," in 2015 IEEE International Conference on Computational Intelligence & Communication Technology. *IEEE*, 202-207. https://doi.org/10.1109/CICT.2015.149

Shukla, R. S. (2022). "IoT Based Designing of Secure Data Storage System in Distributed Cloud System with Big Data using Cryptography Algorithm," in 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART). *IEEE*, 264–270. https://doi.org/10.1109/SMART55829.2022.10047177

Smith, J., & Johnson, K. (2021). *The Impact of Cloud Computing on SME Competitiveness*. International Journal of Business and Information Systems, 28(3), 320-335.

Silverberg, A. (2013). Fully homomorphic encryption for mathematicians. *Women in Numbers 2: Research Directions in Number Theory*, 111-122.

Stallings, W. (2017). *Cryptography and network security: principles and practice*. Pearson.

Suryawanshi, R., & Shelke, S. (2016). "Improving data storage security in cloud environment using public auditing and threshold cryptography scheme," in 2016 International Conference on Computing Communication Control and automation (ICCUBEA). *IEEE*, 1-6. https://doi.org/10.1109/ICCUBEA.2016.7859990

Yang, T., & Yu, B. (2014). "Study of cryptography-based cyberspace data security," in Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT). *IEEE*, 1-7. https://doi.org/10.1109/ICCCNT.2014.6963039