MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/04/21
Aceptado (Accepted): 2025/07/19

Análisis sistemático de protocolos de seguridad de datos en el cloud computing: Revisión de la literatura

Systematic analysis of data security protocols in cloud computing: Literature review

Kevin Zambrano and Denise Vera

***Abstract*—This paper presents a systematic review of relevant studies published between 2019 and 2024, focusing on data security protocols in cloud computing environments. The selection process was based on rigorous criteria to identify the most relevant features of these protocols and their current applications. The review examines their advantages as well as the cryptographic mechanisms used to protect sensitive data, including Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC). Additionally, the increasing use of Kubernetes as a container orchestration tool is analyzed, acknowledging its significance in modern cloud infrastructures. Within this context, several studies are reviewed that highlight implementation limitations such as inadequate privilege management and the reliance on third-party solutions. This research aims to provide a comprehensive understanding of current trends and challenges in cloud data security and to support the identification of potential strategies to address these issues and enhance the robustness of cloud-based security architectures.**

***Index Terms*—Cloud security, security protocols, data encryption, Cloud Computing, Kubernetes.**

***Resumen*—Este trabajo presenta una revisión sistemática de estudios relevantes publicados entre los años 2019 y 2024, centrados en los protocolos de seguridad de datos en entornos de computación en la nube. La selección de artículos se realizó mediante criterios rigurosos, con el objetivo de identificar las características más destacadas de estos protocolos y sus aplicaciones actuales. Se analizan tanto sus ventajas como los mecanismos criptográficos utilizados para proteger la información sensible, entre los que se encuentran AES, RSA y ECC. Adicionalmente, se considera el creciente uso de Kubernetes como herramienta de orquestación de contenedores, reconociendo su importancia dentro de las infraestructuras modernas en la nube. En este contexto, se examinan diversas publicaciones que evidencian limitaciones en su implementación, tales como la gestión inadecuada de privilegios y la dependencia de soluciones de terceros. El estudio ofrece una visión integral que facilite la comprensión de los desafíos actuales y oriente la búsqueda de soluciones que fortalezcan la seguridad en entornos cloud.**

***Palabras Claves*—Seguridad en la nube, protocolos de seguridad, cifrado de datos, computación en la nube, Kubernetes.**

Kevin Zambrano and Denise Vera are with the Facultad de Ciencias Informática, Universidad Tecnica de Manabí, Manabí, Ecuador (e-mail: {kzambrano0732 , denise.vera}@utm.edu.ec).

I. Introducción

El cloud computing es una forma de trabajo que ha transformado los métodos mediante los cuales las empresas procesan, administran y almacenan datos, aprovechando su flexibilidad, escalabilidad y reducción de costos. Este entorno ha permitido la reducción de costos operativos y ha facilitado el acceso a recursos computacionales avanzados sin la necesidad de costear una infraestructura física propia.

Sin embargo, estas compañías enfrentan preocupaciones importantes relacionadas con la seguridad de los datos, debido a la rápida adopción de esta tecnología, la creciente amenaza de ataques informáticos más sofisticados y la posible exposición de datos sensibles en entornos compartidos.

Las amenazas en la seguridad de la nube son diversas, incluyendo el acceso no autorizado, la filtración de datos, ataques de denegación de servicio y la manipulación de información. Estas vulnerabilidades crean brechas en la confidencialidad, integridad y disponibilidad de los datos, lo que crea un gran desafío para las organizaciones que manejan información crítica.

En este contexto, los protocolos de seguridad fueron diseñados para mitigar estos riesgos proporcionando diversas técnicas de autenticación, cifrado y control de acceso que buscan garantizar la protección de los datos en el entorno cloud. A medida que un mayor número de empresas adopta la tecnología en la nube, enfrentan desafíos relacionados con su implementación. Esto genera incertidumbre en las organizaciones sobre la delegación de datos sensibles al entorno cloud, ya que existen muchos riesgos asociados a la privacidad y seguridad [1].

Para reducir esta incertidumbre, se realizó una revisión sistemática de los protocolos de seguridad de datos en el entorno de cloud computing, utilizando la literatura disponible en los últimos años. La gran cantidad de protocolos de seguridad existentes, la variabilidad de su efectividad y los requisitos para su aplicación complican la tarea de seleccionar e implementar la solución más adecuada. Considerando esto, la criptografía es un método ampliamente usado para solidificar la seguridad de la información [2] y suele ser

DOI: 10.24133/maskay.v16i1.4150

incluida como parte integral de varios protocolos.

Este trabajo tuvo como objetivo ofrecer un panorama más amplio sobre los protocolos de seguridad de datos existentes y ofrecer recomendaciones para la mejora de las estrategias actuales y orientar futuras investigaciones en el área. La correcta implementación de medidas de seguridad en la nube es fundamental para garantizar la confianza de las organizaciones y sus usuarios en los servicios cloud, ofreciendo un entorno más seguro y eficiente para el manejo de la información.

Considerando lo mencionado, el estudio analizó de manera sistemática los protocolos de seguridad de datos en el cloud computing, evaluando sus características y técnicas de encriptación utilizadas. Se buscó identificar las estrategias de cifrado más usadas, las principales características de dichos protocolos, así como las limitaciones que presenta la infraestructura basada en Kubernetes dentro del cloud computing. Para ello, se realizó una revisión de la literatura académica reciente, seleccionando estudios relevantes publicados en los últimos cinco años.

II. Trabajos Relacionados

Las amenazas a la seguridad de los datos han impulsado investigaciones en torno a métodos de protección, identificación de vulnerabilidades y aplicación de normativas internacionales como las normas ISO/IEC 27001. Sin embargo, la mayoría de los estudios se han centrado en la seguridad general de la información en la nube, sin profundizar en los protocolos específicos de seguridad de datos. A continuación, se presenta un análisis de investigaciones recientes relacionadas.

En 2020, Kumar y Bhatia, de la Netaji Subhas University of Technology, llevaron a cabo un análisis de diversos métodos para reducir riesgos como la filtración o alteración de datos [3]. Su estudio concluyó que la mejora en la seguridad requiere la incorporación de estrategias innovadoras en la transferencia y almacenamiento de datos, más allá de los métodos tradicionales.

En paralelo, el mismo año, en la Charotar University of Science and Technology, Patel, Shah, Ramoliya y Nayak llevaron a cabo una revisión sobre amenazas, ataques y problemas de seguridad en cloud computing [1]. Identificaron ocho problemas de seguridad, veinte amenazas y once formas de ataque. Señalaron que la rápida adopción del entorno de la nube sin un análisis de riesgos adecuado puede generar vulnerabilidades significativas para las organizaciones.

En 2021, Pérez Reyes llevó a cabo una evaluación sobre seguridad informática en la adopción del cloud computing en la industria alimentaria [4]. Aplicando las normas ISO 2009 y 2013, determinó que existe una relación directa entre la integridad de los datos y los controles de acceso, además de identificar debilidades en la implementación de medidas de seguridad.

En 2020, Torres González realizó un estudio en Bogotá, Colombia, enfocado en los componentes de seguridad implementados por pequeñas y medianas empresas (pymes) que adoptan soluciones de cloud computing [5]. Su estudio encontró que los proveedores de servicios en la nube cuentan con medidas de protección contra alteraciones de datos, suplantación de identidad y ataques de denegación de servicio. Además, subrayó la importancia de que tanto proveedores como clientes implementen planes de recuperación ante desastres y mecanismos de control de acceso.

III. Metodología

Para la presente revisión sistemática de la literatura, se estableció dividir la metodología en tres fases secuenciales: planificación, realización y resultados.

Dicha división facilitó estructurar el proceso de búsqueda, filtrado y análisis de estudios relevantes de manera sistemática y coherente con los objetivos del trabajo.

A. Planificación

Durante esta fase se formularon las preguntas de investigación que guiarían todo el proceso:

- Q1: ¿Cuál es la ventaja del protocolo en específico para asegurar los datos en el cloud computing?
- Q2: ¿Cuáles son las medidas de seguridad con técnicas de cifrado más utilizadas en la protección de datos en cloud computing, según los estudios revisados en los últimos cinco años?
- Q3: ¿Cuáles son las limitaciones que presenta la seguridad de datos en cloud computing en la infraestructura Kubernetes?

A partir de estas preguntas, se establecieron las palabras clave en inglés: “Cloud Computing", "security data”, "data security", "Protocol", "encrypted", "Kubernetes", "K8s", "security", "cloud", "Container". Estas palabras se combinaron para crear dos cadenas de búsqueda que se aplicaron en las bases de datos Scopus y IEEE Xplore. Las combinaciones se diseñaron para maximizar la cobertura temática, empleando operadores booleanos adecuados. Los detalles de las cadenas de búsqueda ejecutadas se presentan en la Tabla I.

Tabla I
Cadenas de búsqueda utilizadas en las bases de datos Scopus e IEEE Xplore para la recopilación de literatura relacionada

Fuente	Primera cadena de búsqueda	Segunda cadena de búsqueda
Scopus	("Cloud Computing" AND ("security data" OR "data security") AND ("Protocol" OR "encrypted"))	("Kubernetes" OR "K8s") AND "security" AND ("cloud" OR "Container")
IEEE Xplore	("Cloud Computing" AND ("security data" OR "data security") AND ("Protocol" OR "encrypted"))	("Kubernetes" OR "K8s") AND "security" AND ("cloud" OR "Container")

Solo se consideraron exclusivamente publicaciones entre 2019 y 2024 y se priorizaron las publicaciones en revistas científicas y actas de conferencias. Los criterios de inclusión y exclusión se detallan a continuación en la Tabla II.

Tabla II

CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN UTILIZADOS PARA FILTRAR LOS ARTÍCULOS RELEVANTES

# Inclusión	# Exclusión
Publicaciones de los últimos 5 años	Análisis o revisión
Ponencias o publicaciones en revistas científicas	Enfoque no relevante al almacenamiento o transferencia de datos
Enfoque en implementación y mejoramiento	Artículo restringido.
elación con el uso de Kubernetes	No relacionado con cloud computing.

B. Realización

Los resultados obtenidos fueron sometidos a filtros conforme a los criterios de inclusión y exclusión definidos en la Tabla II. El proceso se divide en dos etapas, una automatizada basada en criterios del idioma, disponibilidad del artículo y tipo de documento. La segunda etapa fue manual, donde se incluyó una lectura preliminar de título, resumen y palabras clave para evaluar la relación temática de los estudios.

Los estudios preseleccionados fueron analizados en mayor profundidad en la introducción, metodología y conclusiones. Este procedimiento permitió una depuración progresiva, lo que redujo el total inicial de 4132 artículos a una muestra final de 43 estudios relevantes. Este proceso se detalla en la Tabla III y en la Fig. 1.

TABLA III
PROCESO DE FILTRADO DE ARTÍCULOS DESDE LA BÚSQUEDA INICIAL HASTA LA SELECCIÓN FINAL

Scopus	IEEE Xplore	Descripción
1354	2778	Ejecución de las cadenas de búsqueda
961	1694	Filtros (año, idioma, tipo de documento)
151	310	Filtro resumen, título, palabras clave y criterios de inclusión y duplicados.
22	21	Filtro introducción, metodología y conclusiones.

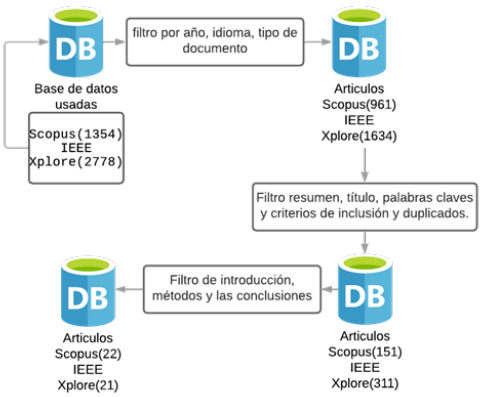

Fig. 1. Proceso de selección de artículos desde la búsqueda inicial hasta la muestra final de estudios relevantes. Visualización basada en los datos de la Tabla III.

En la Fig. 2 se muestra el total de artículos recuperados en la búsqueda. Se observa que en IEEE se encontraron mayor cantidad de artículos, esto debido a la especialización de la base de datos en la tecnología, mientras que en Scopus el total de resultados es más de la mitad de los encontrados en IEEE Xplore.

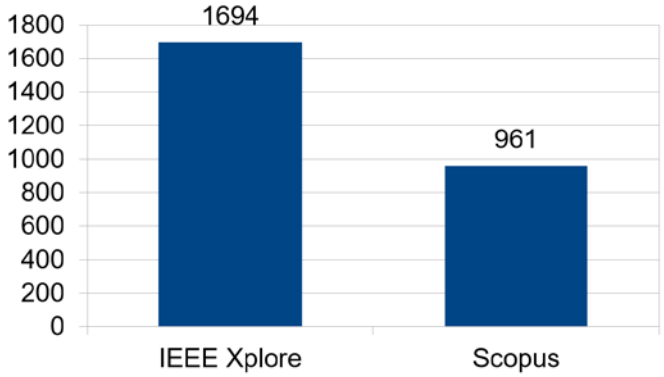

Fig. 2. Comparativa del total de artículos encontrados por base de datos.

La Fig. 3 muestra la tendencia de publicación por año de los artículos encontrados. Se puede observar cómo las publicaciones desde 2020 tienden a subir hasta 2024, donde se presenta una bajada en las publicaciones, lo cual puede atribuirse a la fecha en la que se realizó la búsqueda, que fue antes de la finalización del año 2024.

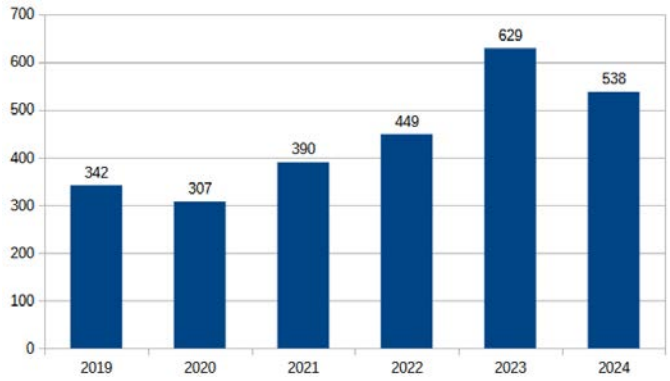

Fig. 3. Tendencia anual de publicaciones encontradas. Se evidencia un aumento progresivo hasta 2023, con una caída parcial en 2024 atribuible al momento de cierre de la búsqueda.

En la Tabla IV se aprecia el cambio de los potenciales estudios del período de tiempo de 2019 a 2024, a los que se usaron para el trabajo.

TABLA IV
NÚMERO DE ARTÍCULOS POTENCIALES Y SELECCIONADOS POR BASE DE DATOS. REFLEJA EL RESULTADO DEL PROCESO DE FILTRADO APLICADO A SCOPUS E IEEE XPLORE

Fuente	Estudios potencialmente elegibles	Estudios seleccionados
Scopus	961	22
IEEE Xplore	1634	21

La Fig. 4 muestra cómo la cantidad de artículos seleccionados después de aplicar los filtros, criterios de

exclusión y revisión de los artículos, lo cual resultó en una selección final de 22 artículos de Scopus y 21 de IEEE Xplore.

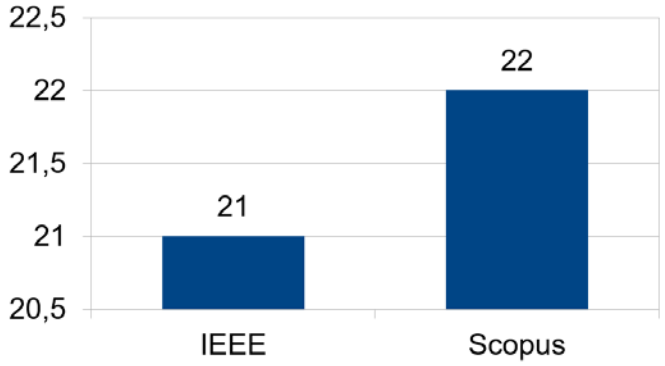

Fig. 4. Distribución final de los 43 artículos seleccionados por base de datos. Scopus e IEEE aportaron proporciones similares.

La Fig. 5 presenta cómo los artículos seleccionados tendieron a disminuir con el paso de los años desde su publicación original, lo que no implica que los artículos recientes sean menos relevantes, sino que no se ajustaban a los objetivos del estudio.

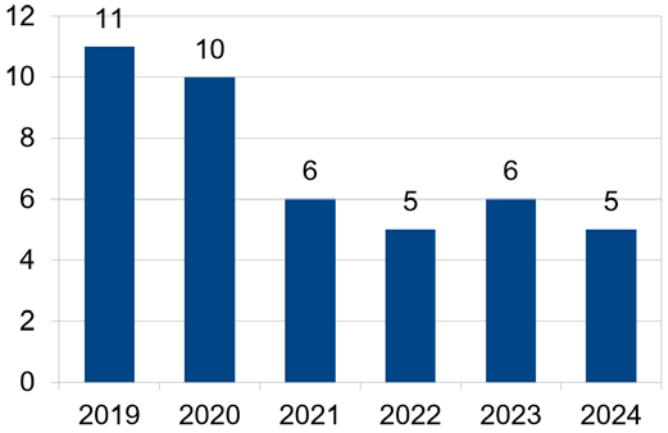

Fig. 5. Evolución anual de los artículos seleccionados. Se observa menor presencia de estudios recientes, sin que ello implique una menor relevancia científica.

C. Resultados

La muestra final de los 43 artículos se utilizó para responder las tres preguntas de investigación. Para Q1 se identificaron y clasificaron protocolos de seguridad en cloud computing según sus características. En Q2, se extrajeron las técnicas de cifrado empleadas y su frecuencia de uso. Finalmente, para Q3, se revisaron estudios que abordaron limitaciones en Kubernetes, permitiendo consolidar un conjunto de vulnerabilidades comunes. Este proceso está desarrollado de forma más clara en la Sección IV.

IV. Resultados

Q1. ¿Cuál es la ventaja del protocolo en específico para asegurar los datos en el cloud computing?

Tabla V

Protocolos de seguridad analizados y sus características, organizadas según: detección de seguridad, control de acceso, privacidad, integridad, resistencia a ataques y descentralización

Protocolo	c1	c2	c3	c4	c5	c6
[6]		✓		✓	✓	
[7]		✓	✓	✓	✓	
[8]		✓	✓		✓	
[9]		✓	✓	✓	✓	✓
[10]		✓	✓	✓	✓	
[11]				✓	✓	
[12]	✓			✓	✓	
[13]		✓	✓		✓	
[14]		✓		✓	✓	
[15]		✓	✓		✓	✓
[16]		✓	✓			
[17]		✓	✓		✓	
[18]		✓	✓			

c1=Detección de seguridad, c2=Control de acceso, c3=Anonimato y Privacidad, c4=Integridad de datos, c5=Resistencia a ataque, c6=Descentralizado

Como se puede observar en la TABLA V en el análisis de 13 protocolos identificados [6]-[18].

Siguiendo el orden de la TABLA V los protocolos incluidos son protocolo de intercambio seguro de datos médicos en el entorno de WBAN asistido por la nube, protocolo de seguridad de datos para terceros de confianza semiautorizados (ADSS), protocolo de autenticación robusta para infraestructura de salud en la nube basada en iomt (RAPCHI), protocolo de ias basado en blockchain, autenticación de servicios inteligentes (SSA), protocolo eficiente de intersección privada de conjuntos para entornos en la nube, Sec-Manage, protocolo ligero y seguro para sistemas de salud electrónica (LSP–eHS), protocolo de preservación de privacidad en nube con EDAC-MAC, agrupamiento y gestión multiagencia, construcción de un protocolo de acuerdo de claves para infraestructura médica en la nube utilizando blockchain (CKMIB), protocolo de gestión de claves de grupo de intercambio de secretos (SSGK), protocolo de clasificación SVM privado en la nube, Control de Acceso Distribuido anónimo finamente granular con decifrado verificable en la nube pública (VOD-ADAC),

Se puede destacar que el protocolo llamado Sec-Manage [12] incorpora una técnica para implementar detección de seguridad; el protocolo emplea un modelo de interacción basado en políticas, el cual establece cómo deben interactuar las entidades en el entorno cloud. Esto permite supervisar las interacciones en tiempo real y detectar comportamientos anómalos. Además, esta capacidad permite mantener la integridad de los datos y proporciona resistencia a ciertos ataques maliciosos.

Once de los protocolos: [6], [7], [8], [9], [10], [13], [14], [15], [16], [17], [18], ofrecen mecanismos de control de acceso. Nueve protocolos analizados [7], [8], [9], [10], [13], [15], [16], [17], [18] implementan o proponen técnicas o procesos para asegurar el anonimato y la privacidad de los usuarios. Siete [6], [7], [9], [10], [11], [12], [14] incluyen métodos para mantener la integridad de los datos.

Este aspecto es clave, junto con el control de acceso y la

privacidad, para entornos de salud, donde solo el paciente y el médico tratante deben tener acceso.

De los protocolos analizados, once [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [17] proporcionan resistencia a uno o varios tipos de ataques maliciosos externos o internos como se puede ver en la Tabla VI a continuación.

TABLA VI
PROTOCOLOS DE SEGURIDAD Y SU RESISTENCIA A DIVERSOS ATAQUES ORGANIZADOS POR EXTERNOS E INTERNOS

Protocolo	Ataques de seguridad							
	Externos					Internos		
	a1	a2	a3	a4	a5	a6	a7	a8
[6]	✓	✓	✓	✓	✓		✓	✓
[7]	✓	✓	✓	✓	✓			
[8]	✓	✓	✓	✓	✓	✓	✓	✓
[9]	✓	✓	✓		✓		✓	✓
[10]	✓	✓	✓	✓	✓			
[11]	✓	✓						
[12]	✓	✓			✓			✓
[13]	✓	✓	✓		✓	✓		✓
[14]	✓	✓	✓	✓	✓			
[15]	✓	✓	✓	✓	✓	✓	✓	✓
[17]					✓			

a1 =Intercepción, a2 =Repetición de mensajes, a3 = Man-in-the-middle, a4 = Divulgación de clave de sesión, a5 =Frescura de clave y secreto perfecto hacia adelante, a6 = Ataque interno, a7 =Fuga de seguridad efímera a8 =Ataques relacionados con secretos compartidos y parámetros del protocolo

Dos de los protocolos [9], [15] tienen aspectos descentralizados mediante tecnología blockchain.

En situaciones específicas, los protocolos otorgan sólo un marco general, lo que permite la implementación o personalización. Por ejemplo, el protocolo de intercambio seguro de datos médicos en el entorno de WBAN asistido por la nube [6], el cual recomienda el uso de una clave simétrica para el cifrado y descifrado.

Se observa que los principales aspectos que un protocolo de seguridad de datos en el cloud computing priorizan mantener un control de acceso a los datos, la privacidad mediante anonimato de los datos, la integridad frente a cambios no autorizados y la resistencia a los ataques tanto externos como internos.

Q2. ¿Cuáles son las medidas de seguridad con técnicas de cifrado más utilizadas en la protección de datos en cloud computing, según los estudios revisados en los últimos cinco años?

En los estudios analizados se reporta el uso de diversas técnicas de cifrado, tanto simétricas como asimétricas, empleadas para garantizar la seguridad de los datos en entornos de computación en la nube.

A continuación, se describe cada técnica, considerando su funcionamiento general, aplicación y frecuencia de uso en los artículos revisados.

TABLA VII
TÉCNICAS DE ENCRIPTADO IDENTIFICADAS EN LOS ESTUDIOS REVISADOS. SE DETALLAN EL TIPO DE CIFRADO, NÚMERO DE ESTUDIOS EN LOS QUE SE UTILIZAN Y LAS FUENTES CORRESPONDIENTES

#	Encriptación	Número de usos	Fuentes
1	Asimétricos no especificados	2	[8],[19]
2	Simétricos no especificados	4	[18],[6], [8], [9]
3	Hash	3	[8], [13], [18]
4	AES (Advanced Encryption Standard)	1	[16]
5	Cifrado homomórfico	2	[11],[17]
6	RSA	2	[10],[16]
7	3DES	1	[14]
8	Elliptic Curve Cryptography (ECC)	3	[13],[15],[10]
9	Hyper Elliptic Curve Cryptography (HECC)	1	[9]
10	Identity-based encryption	1	[17]
11	proxy re-encryption	1	[6]
12	Attribute-Based Encryption (ABE)	2	[18],[20]
13	Simétricos totales	6	[18],[6], [8], [19],[14],[16]
14	Asimétricos totales	11	[8],[19],[13],[15],[10],[9],[18],[20],[10],[16],[17]

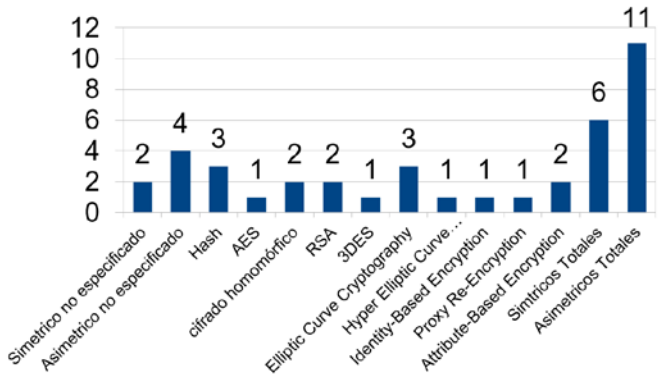

Fig. 6. Técnicas de encriptación representadas en barras según el total de veces implementadas en los estudios analizados.

AES (Advanced Encryption Standard) es un algoritmo de cifrado simétrico ampliamente adoptado por su eficiencia, velocidad y nivel de seguridad. Resulta especialmente adecuado para el cifrado de grandes volúmenes de datos. Fue reportado en el estudio [16], donde se empleó para proteger la información almacenada en entornos cloud.

RSA (Rivest-Shamir-Adleman) constituye uno de los algoritmos de cifrado asimétrico más ampliamente utilizados en entornos de seguridad digital. Se basa en la dificultad computacional de factorizar grandes números primos y se emplea con frecuencia para el intercambio seguro de claves en arquitecturas distribuidas. Su uso fue identificado en dos de los estudios revisados [10], [16].

ECC (Elliptic Curve Cryptography) es un método de cifrado asimétrico que ofrece altos niveles de seguridad utilizando claves de menor longitud, lo que lo convierte en una opción eficiente en términos de rendimiento. Esta técnica fue empleada en tres de los estudios revisados [10], [13], [15].

HECC (Hyper Elliptic Curve Cryptography) es una variante de ECC que utiliza curvas hiperelípticas para ofrecer una

mayor complejidad matemática y, potencialmente, una mayor seguridad. Se identificó en un único estudio [9].

3DES (Triple Data Encryption Standard) representa una evolución del algoritmo DES, en la cual el proceso de cifrado se aplica tres veces consecutivas sobre cada bloque de datos, lo que incrementa la robustez frente a ataques de fuerza bruta. Aunque ofrece un nivel de seguridad superior al de su predecesor, presenta desventajas significativas en términos de eficiencia y rendimiento frente a algoritmos más modernos, como AES. Esta técnica fue reportada en un estudio [14].

El cifrado homomórfico permite realizar operaciones matemáticas directamente sobre datos cifrados sin necesidad de desencriptarlos previamente, lo cual resulta especialmente útil en contextos donde se requiere preservar la confidencialidad durante el procesamiento de datos. Esta técnica fue mencionada en dos estudios [11], [17].

Las funciones hash se utilizaron de manera complementaria a otros esquemas de cifrado con el fin de asegurar la integridad de los datos. Su implementación fue identificada en tres estudios [8], [13], [18].

Attribute-Based Encryption (ABE) es una técnica de cifrado asimétrico que permite establecer políticas de acceso detalladas basadas en atributos específicos del usuario. De esta forma, se ofrece un mayor control sobre quién puede acceder a determinados datos. Se identificó en dos estudios [18], [20].

Identity-Based Encryption (IBE) permite generar claves públicas a partir de la identidad del usuario, lo cual simplifica la gestión de certificados y facilita la distribución de claves. Esta técnica fue mencionada en un estudio [17].

Proxy Re-Encryption es un mecanismo mediante el cual un tercero autorizado puede transformar un mensaje cifrado para que sea accesible por un nuevo destinatario, sin necesidad de revelar el contenido original. Fue identificada en un estudio [6].

También se identificaron varios estudios [6], [8], [9], [18], [19] en los que se alude al uso de técnicas de cifrado simétrico o asimétrico sin especificar. En estos casos, los autores se limitaron a señalar el uso de cifrado de forma general, lo que indica flexibilidad en la elección de la técnica, determinada por los requisitos específicos del entorno de aplicación.

En conjunto, las técnicas identificadas reflejan una diversidad de enfoques y soluciones tecnológicas orientadas a fortalecer la seguridad de los datos en el contexto de la computación en la nube, especialmente en lo que respecta a la confidencialidad, integridad y control de acceso. El uso recurrente de algoritmos como ECC, RSA y ABE indica una tendencia hacia mecanismos criptográficos robustos, eficientes y adaptables a distintos escenarios de implementación.

Para concluir las dos primeras preguntas, a continuación, se presenta una tabla sintetizada con los estudios analizados correspondientes a las dos primeras preguntas de investigación, Q1 y Q2, donde se resumen las técnicas de cifrado usadas y las características reforzadas o agregadas en el estudio.

TABLA VIII

ESTUDIOS ANALIZADOS, TÉCNICAS DE CIFRADO IMPLEMENTADAS Y ASPECTOS REFORZADOS

Fuente	Técnicas de cifrado implementadas
[6]	Cifrado simétrico no especificado, Proxy re-encryption
[7]	No aplica.
[8]	Hash, Asimétrico no especificado, Simétrico no especificado
[9]	Simétrico no especificado, Hyper Elliptic Curve Cryptography (HECC)
[10]	Elliptic Curve Cryptography (ECC), RSA
[11]	Cifrado homomórfico
[12]	No aplica
[13]	Elliptic Curve Cryptography (ECC), Hash.
[14]	3DES
[15]	Elliptic Curve Cryptography (ECC)
[16]	AES (Advanced Encryption Standard), RSA
[17]	Cifrado homomórfico, Identity-based encryption
[18]	Simétricos no especificado, Attribute-Based Encryption (ABE)
[19]	Asimétricos no especificado,
[20]	Attribute-Based Encryption (ABE)

Q3. ¿Cuáles son las limitaciones que presenta la seguridad de datos en cloud computing en la infraestructura Kubernetes?

TABLA IX

COMPILACIÓN DE DEBILIDADES TÉCNICAS IDENTIFICADAS EN ESTUDIOS RECIENTES SOBRE KUBERNETES

Fuente	Limitación encontrada
[19]	Falta de soporte para cifrado
[21]	Seguridad de la Infraestructura Compartida
[22]	Sustitución de imágenes de contenedor
[23]	Abuso de privilegios
[24]	Dependencia de Soluciones de Terceros
[25]	Dependencia de Soluciones de Terceros
[26]	Abuso de privilegios
[27]	Complejidad en la Gestión Global
[28]	Limitaciones en la monitorización
[29]	Dependencia de Soluciones de Terceros
[30]	Limitaciones en la monitorización
[31]	Contención de Memoria de Enclave
[32]	Seguridad de la Infraestructura Compartida
[33]	Seguridad de la Infraestructura Compartida, Contención de Memoria de Enclave
[34]	Inconsistencias en la Configuración de Seguridad
[35]	Distribución desigual de carga
[36]	Asignación estática de recursos
[37]	Asignación estática de recursos
[38]	Abuso de privilegios
[39]	Limitaciones en la monitorización
[40]	Dependencia de Soluciones de Terceros
[41]	Configuraciones Inseguras por Defecto
[20]	Abuso de privilegios
[42]	Configuraciones Inseguras por Defecto
[43]	Enfoque Reactivo en Seguridad
[44]	Dependencia de Soluciones de Terceros, Seguridad de la Infraestructura Compartida
[45]	Inconsistencias en la Configuración de Seguridad
[46]	Sustitución de imágenes de contenedor, Gestión de contenedores infectados
[47]	Configuraciones Inseguras por Defecto
[48]	Configuraciones Inseguras por Defecto, Abuso de privilegios
[49]	Configuraciones Inseguras por Defecto

En el análisis basado en los problemas que las propuestas de los artículos buscaron resolver, se identificaron múltiples

limitaciones, desafíos o problemas que afectan la seguridad de datos en Kubernetes los cuales se en listan a continuación:

Falta de soporte para cifrado, infraestructura compartida, abuso de privilegios, dependencia de soluciones de terceros, complejidad en la gestión global, limitaciones en la monitorización, contención de memoria de enclave, seguridad de la infraestructura compartida, asignación estática de recursos, inconsistencias en la configuración de seguridad.

Los más mencionados son la dependencia de soluciones de terceros y la configuración insegura por defecto, abuso de privilegios, infraestructura compartida.

El estudio realizado por Stoyanov et al. [19] señala cómo los checkpoints generados por defecto en Kubernetes no están encriptados y para esto se usa una herramienta de CRIU (Checkpoint/Restore In Userspace) para congelar el estado del contenedor y cifrarlo de forma que se aseguran los datos.

En el estudio donde se aborda los riesgos de la seguridad en las nubes basadas en contenedores, específicamente cómo las llamadas a un sistema vulnerable pueden ser explotadas por contenedores maliciosos, se identifica el problema del vecino ruidoso (noisy neighbor) [21], en el que múltiples usuarios comparten el mismo cluster y generan llamadas al sistema vulnerable que pueden interferir entre sí, abriendo vectores de ataques a nivel de sistema.

Los estudios realizados por Pecka et al. [23] y Santos et al. [48] expresan una preocupación por un posible abuso de privilegios en un entorno de Kubernetes ya sea mediante el despliegue de programas maliciosos o la acumulación de cargas de trabajo privilegiado que deja expuestos los datos con los que se trabaja. Estas situaciones se relacionan con un pobre aislamiento entre contenedores, que se puede mitigar poniendo políticas de comunicación más estrictas entre los elementos orquestados por Kubernetes.

Por su parte, Bringhenti et al. [27] menciona que en los entornos que ejecutan programas en paralelo, dificulta la gestión global y que, si no se hace de forma adecuada, crea brechas de seguridad. Esto evidencia cómo la escalabilidad, aunque ventajosa, también introduce retos en cuanto a coordinación y aislamiento.

El estudio de Lim et al. [25] destaca que Kubernetes no dispone de un mecanismo nativo para gestionar el ciclo de vida de las máquinas virtuales. Lo que obliga a recurrir a soluciones externas, como las que ofrece la plataforma OpenStack para la creación y gestión de entornos en la nube.

El estudio donde Karn et al. [49] documenta configuraciones predeterminadas inseguras que otorgan privilegios elevados a los contenedores, lo cual amplifica el riesgo de escalamiento de privilegios si no se controlan con políticas de acceso estrictas.

También se mencionan limitaciones como la falta de migración de procesos en vivo, gestión de versiones y problemas en la asignación de recursos. Estas limitaciones son incluidas como parte de la dependencia de soluciones de terceros.

Cabe destacar que una buena parte de las limitaciones existentes pueden mitigarse con herramientas externas y un cuidado adecuado de las políticas de aislamiento, pero esto refuerza el problema original, ya que la seguridad de Kubernetes depende en gran medida de soluciones de terceros, lo que puede convertirse en una fuente adicional de riesgo si dichas herramientas no están correctamente integradas ni validadas.

Finalmente, la Tabla IX muestra la recurrencia en la que se encontraron las limitaciones de Kubernetes

TABLA X
RECURRENCIA DE LIMITACIONES ENCONTRADAS EN LA INFRAESTRUCTURA KUBERNETES SEGÚN LOS ESTUDIOS REVISADOS

Limitación encontrada	Veces encontrada	Fuente
Falta de soporte para cifrado	1	[19]
Seguridad de la Infraestructura Compartida	4	[21], [32], [33], [44]
Sustitución de imágenes de contenedor	2	[22], [46]
Abuso de privilegios	5	[20], [23], [26], [38], [48]
Dependencia de Soluciones de Terceros	5	[24], [25], [29], [40], [44]
Complejidad en la Gestión Global	1	[27]
Limitaciones en la monitorización	3	[28], [30], [39]
Contención de Memoria de Enclave	2	[31], [33],
Inconsistencias en la Configuración de Seguridad	2	[34], [45]
Distribución desigual de carga	1	[35]
Asignación estática de recursos	2	[36], [37]
Configuraciones Inseguras por Defecto	5	[41], [42], [47], [48], [49]
Enfoque Reactivo en Seguridad	1	[43]
Gestión de contenedores infectados	1	[46]

V. DISCUSIÓN

El análisis de los protocolos de seguridad de datos en cloud computing evidencia avances significativos en aspectos como el control de acceso y la integridad de los datos, logrados mediante el uso de tecnologías emergentes como la blockchain.

Aun así, se presentan oportunidades de mejora, particularmente en el monitoreo preventivo de anomalías, como se señala en el trabajo de Farahmandian et al. [12], previniendo ataques externos o comprometer la integridad de los datos. El uso de blockchain como herramienta para evitar el acceso no autorizado o la modificación de los datos es prometedor; sin embargo, la dificultad que presenta su implementación y sus altos costos asociados desalienta la normalización de su uso.

Respecto a la segunda pregunta de investigación, entre las técnicas criptográficas analizadas, ECC destaca por ofrecer un alto nivel de seguridad con claves más cortas, lo que mejora la eficiencia. A pesar de esto, su implementación enfrenta obstáculos relacionados con la compatibilidad con sistemas, lo que restringe su adopción en infraestructuras existentes.

En contraste, ABE permite definir políticas de acceso detalladas basadas en atributos, lo que proporciona

flexibilidad en la gestión de datos confidenciales, aunque presenta mayor complejidad operativa y coste computacional.

Por su parte, RSA, a pesar de su amplia adopción, presenta desventajas en términos de rendimiento, especialmente en entornos que requieren alta escalabilidad, como los entornos cloud. Estas diferencias reflejan que no existe una solución universal, y que la elección del protocolo debe estar alineada con las necesidades técnicas y operativas de cada caso.

Además, se identificó el uso de cifrado homomórfico y proxy re-encryption como mecanismos avanzados, que permiten preservar la confidencialidad sin sacrificar flexibilidad. No obstante, estos enfoques suelen implicar una carga computacional elevada, lo que limita su adopción en entornos productivos. Asimismo, varios artículos no especifican la técnica de cifrado utilizada, lo que refleja una flexibilidad intencionada en la integración de algoritmos criptográficos.

En el caso de Kubernetes, si bien proporciona ventajas en la escalabilidad y gestión de recursos, existen vulnerabilidades que lo acompañan. Las configuraciones por defecto inseguras facilitan el abuso de privilegios y una exposición de los datos sensibles.

Cabe mencionar que otra limitación frecuente es la dependencia de herramientas externas para la monitorización, dado que la supervisión nativa de Kubernetes se considera insuficiente por varios autores. Esta dependencia aumenta los posibles puntos de fallo. No obstante, se destaca que muchos de los problemas encontrados se pueden atribuir a la dependencia de soluciones de terceros. Existen herramientas que solucionan y facilitan lidiar con las limitaciones presentadas por Kubernetes, pero esto genera vulnerabilidades si no se seleccionan herramientas confiables.

En consecuencia, resulta fundamental avanzar en el desarrollo de mecanismos de seguridad nativos para Kubernetes, así como en la estandarización de configuración segura que reduzcan la necesidad de herramientas externas.

También se observó la ausencia de pruebas comparativas de rendimiento de las técnicas de cifrado en entornos orquestados con Kubernetes. Realizar evaluaciones en este tipo de entornos sería clave, proporcionando resultados relevantes que podrían orientar el desarrollo de futuros protocolos de seguridad adaptados a plataformas distribuidas.

En conjunto, los hallazgos indican que la seguridad en el cloud computing requiere un enfoque integral que combine múltiples estrategias y tecnologías para hacer frente a los riesgos actuales.

En este sentido, futuras investigaciones podrían centrarse en la adaptación de algoritmos de cifrado en entornos cloud orquestados, en análisis comparativo o en el desarrollo de soluciones integradas que refuercen el aislamiento entre contenedores, y optimicen el monitoreo sin comprometer el rendimiento del sistema.

VI. Conclusiones

El presente análisis sistemático de los protocolos de seguridad de datos en cloud computing permitió identificar las principales estrategias utilizadas para garantizar la protección de la información. Se evidenció la existencia de múltiples protocolos con características específicas, cuyo grado de efectividad depende del contexto de implementación y del nivel de riesgo asumido.

Uno de los hallazgos más relevantes encontrados es el uso creciente de los algoritmos de encriptado asimétricos y, en menor medida, simétricos, para asegurar los datos en su transferencia y almacenamiento, como el encriptado ECC, RSA y ABE. También se identificó el uso de características y técnicas como el cifrado homomórfico o el empleo de proxy de re-encriptado, que proporcionan una capa adicional de seguridad y flexibilidad en la gestión de acceso, lo cual contribuye a un control más seguro de los datos.

Se le identificaron en Kubernetes limitaciones relacionadas con el abuso de privilegios, configuraciones inseguras por defecto y la dependencia de soluciones de terceros. Esto demuestra la necesidad de fortalecer la personalización de la seguridad en los entornos de orquestación de contenedores, así como de seleccionar cuidadosamente las herramientas empleadas y contar con personal técnico capacitado.

Según los hallazgos, las organizaciones deben adoptar protocolos de seguridad adecuados según su contexto específico, nivel de riesgo y su capacidad operativa. Tecnologías como blockchain pueden ser útiles para garantizar trazabilidad y resistencia frente a ataques, pero se requiere avanzar en soluciones más accesibles y menos costosas para su adopción generalizada.

Entre las recomendaciones clave que surgen de este estudio, se destacan:

- Diseñar protocolos de seguridad ligeros pero robustos, adaptables a entornos distribuidos y orquestados.
- Validar empíricamente los protocolos en plataformas reales como Kubernetes.
- Mejorar la integración nativa de herramientas de monitoreo y control dentro del ecosistema Kubernetes.
- Desarrollar estándares para la evaluación comparativa de técnicas criptográficas bajo métricas comunes de rendimiento, consumo de recursos y resistencia a ataques.
- Fomentar el uso combinado de tecnologías como mecanismos complementarios y no excluyentes.

En conclusión, la seguridad en cloud computing continúa representando un desafío que exige un enfoque dinámico. La constante evolución de amenazas e innovación tecnológica requiere la adopción de soluciones contextualmente adecuadas. En este contexto, la adopción de protocolos robustos y adaptativos es clave para mitigar los riesgos y fortalecer la protección de los datos en la nube.

Referencias

[1] A. Patel, N. Shah, D. Ramoliya and A. Nayak, "A detailed review of Cloud Security: Issues, Threats & Attacks," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 758-764, 2020, doi: 10.1109/ICECA49313.2020.9297572.

[2] Sinchana, M.K., Savithramma, R.M, " Survey on Cloud Computing Security" Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, Springer, Singapore, vol 103, pp 1-6, https://doi.org/10.1007/978-981-15-2043-3_1

[3] R. Kumar and M. P. S. Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability," 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, pp. 334-337, 2020, doi: 10.1109/GUCON48875.2020.9231255.

[4] P. R. Tomás Gabriel, "Seguridad Informática en la Adopción de Cloud Computing en la Industria Alimentaria", Rev. Boaciencia. Negocios Tecnol., vol. 1, n.º 2, p. 93, 2021.

[5] A. M. Torres González, "Análisis de los componentes de seguridad informática en la implementación de cloud computing en pequeñas y medianas empresas colombianas", Monografía, UNIVIERSIDAD. NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLGÍA E INGENIERÍA., Bogotá, 2020.

[6] J. Liu, Q. Zhong, R. Sun, X. Du and M. Guizani, "A Secure and Efficient Medical Data Sharing Protocol for Cloud-Assisted WBAN" in 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014307.

[7] P. Zhang, H. Chi, J. Wang, and Y. Shang, "Data security protocol with blind factor in cloud environment" in Information, vol. 12, no. 9, art. no. 340, 2021, doi: 10.3390/info12090340.

[8] V. Kumar, M. S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, and A. Kumari, "RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure" in The Journal of Supercomputing, vol. 78, no. 14, pp. 16167–16196, 2022, doi: 10.1007/s11227-022-04513-4.

[9] S. N. Prasad and C. Rekha, "Blockchain-based IAS protocol to enhance security and privacy in cloud computing," in Measurement: Sensors, vol. 28, art. no. 100813, 2023, doi: 10.1016/j.measen.2023.100813.

[10] B. D. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud-based medical healthcare systems using internet of medical things," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 346–360, 2021, doi: 10.1109/jsac.2020.3020599.

[11] O. Ruan, X. Huang and H. Mao, "An efficient private set intersection protocol for the cloud computing environments," in 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2020, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00053.

[12] S. Farahmandian and D. B. Hoang, "A policy-based interaction protocol between software defined security controller and virtual security functions," in 2020 4th Cyber Security in Networking Conference (CSNet), 2020,doi: 10.1109/CSNet50428.2020.9265460.

[13] A. Delham Algarni, F. Algarni, S. Ullah Jan and N. Innab, "LSP–eHS: A lightweight and secure protocol for e-healthcare system," IEEE Access: Practical Innovations, Open Solutions, vol. 12, pp. 156849–156866, 2024, doi: 10.1109/access.2024.3477922.

[14] S. S. Manivannan, P. Shashidhar, C. Vanmathi and P. M. D. R. Vincent, "Multi authority privacy preserving protocol in cloud computing authentication using grouping algorithm and EDAC-MAC" in 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2019 doi: 10.1109/ICICICT46008.2019.8993380.

[15] S. Itoo, A. A. Khan, V. Kumar, A. Alkhayyat, M. Ahmad and J. Srinivas, "CKMIB: Construction of key agreement protocol for cloud medical infrastructure using blockchain" IEEE Access: Practical Innovations, Open Solutions, vol. 10, pp. 67787–67801, 2022, doi: 10.1109/access.2022.3185016.

[16] S. Han, K. Han and S. Zhang, "A data sharing protocol to minimize security and privacy risks of cloud storage in big data era" in IEEE Access: Practical Innovations, Open Solutions, vol. 7, pp. 60290–60298, 2019, doi: 10.1109/access.2019.2914862.

[17] J. Liang, Z. Qin, J. Ni, X. Lin and X. Shen, "Efficient and Privacy-Preserving Outsourced SVM Classification in Public Cloud," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761610.

[18] H. Wang, D. He and J. Han, "VOD-ADAC: Anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud" in IEEE Transactions on Services Computing, vol. 13, no. 3, pp. 572–583, 2020, doi: 10.1109/tsc.2017.2687459.

[19] R. Stoyanov, A. Reber, D. Ueno, M. Clapiński, A. Vagin and R. Bruno, "Towards efficient end-to-end encryption for container checkpointing systems." in Proceedings of the 15th ACM SIGOPS Asia-Pacific Workshop on Systems, pp. 60–66. 2024. DOI: 10.1145/3678015.3680477.

[20] M. Femminella, M. Palmucci, G. Reali, and M. Rengo, "Attribute-based management of secure Kubernetes cloud bursting." un IEEE Open Journal of the Communications Society, vol. 5, pp. 1276–1298, 2024, doi: 10.1109/ojcoms.2024.3367461.

[21] M. V. Le, S. Ahmed, D, Williams and H. Jamjoom, "Securing container-based clouds with syscall-aware scheduling." in Proceedings of the ACM Asia Conference on Computer and Communications Security, pp. 812–826. 2023 . DOI: 10.1145/3579856.3582835.

[22] A. Sadiq, H. J. Syed, A. A. Ansari, A. O. Ibrahim, M. Alohaly and M. Elsadig, "Detection of Denial of service attack in cloud based Kubernetes using eBPF." in Applied Sciences (Basel, Switzerland), 13(8), p 4700. 2023. DOI: 10.3390/app13084700.

[23] N. Pecka, L. Ben Othmane and A. Valani, "Privilege escalation attack scenarios on the DevOps pipeline within a Kubernetes environment." in Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering, pp 45–49.2022 .DOI: 10.1145/3529320.3529325.

[24] J. Mahboob, and J. Coffman, "A Kubernetes CI/CD pipeline with asylo as a trusted execution environment abstraction framework." in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). 2021. DOI: 10.1109/CCWC51732.2021.9376148.

[25] H. Lim, Y. Kim and K. Sun, "Service management in virtual machine and container mixed environment using service mesh." in 2021 International Conference on Information Networking (ICOIN). 2021. DOI: 10.1109/ICOIN50884.2021.9333888.

[26] S. Shringarputale, P. McDaniel, K. Butler and T. La Porta, "Co-residency Attacks on Containers are Real." in Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop. 2020. DOI: 10.1145/3411495.3421357.

[27] D. Bringhenti, G, Marchetto, R. Sisto, F. Valenza and J. Yusupov, "Introducing programmability and automation in the synthesis of virtual firewall rules." in 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, DOI: 10.1109/NetSoft48620.2020.9165434.

[28] A. F. Baarzi, G. Kesidis, D. Fleck and A. Stavrou, "Microservices made attack-resilient using unsupervised service fissioning." Proceedings of the 13th European Workshop on Systems Security, 2020, DOI: 10.1145/3380786.3391395.

[29] A. Borisova, V. Shvetcova, and O. Borisenko, "Adaptation of the TOSCA standard model for the Kubernetes container environment," in 2020 Ivannikov Memorial Workshop (IVMEM), 2020. DOI: 10.1109/IVMEM51402.2020.00008.

[30] T. Heo, J. H. An, and Y. Kim, "Design and implementation of migration manager between cloud edge platforms," in Proceedings of the International Conference on Research in Adaptive and Convergent Systems, 2020. DOI: 10.1145/3400286.3418279.

[31] D. Y. Yuan, and T. Wildish, "Bioinformatics application with Kubeflow for batch processing in clouds," in Lecture Notes in Computer Science, Springer International Publishing, 2020, pp. 355–367. DOI: 10.1007/978-3-030-59851-8_24.

[32] A. Brito, C. Fetzer, S. Köpsell, P. Pietzuch, M. Pasin, P. Felber, K. Fonseca, M. Rosa, L. Gomes Jr, R. Riella, C. Prado, L. F. Rust, D. E. Lucani, M. Sipos, L. Nagy and M. Fehér, "Secure end-to-end processing of smart metering data," in Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, no. 1, 2019. DOI: 10.1186/s13677-019-0141-z.

[33] N. Surantha and F. Ivan, "Secure Kubernetes networking design based on zero trust model: A case study of financial service enterprise in Indonesia," in Innovative Mobile and Internet Services in Ubiquitous Computing, Springer International Publishing, pp. 348–361. 2020. DOI: 10.1007/978-3-030-22263-5_34.

[34] G. P. Fernandez and A. Brito, "Secure container orchestration in the cloud: Policies and implementation," in Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 1635–1642. 2019. DOI: 10.1145/3297280.3297296.

[35] B. Thurgood and R. G. Lennon, "Cloud computing with Kubernetes cluster elastic scaling," in Proceedings of the 3rd International

Conference on Future Networks and Distributed Systems, pp. 1–6. 2019. DOI: 10.1145/3341325.3341995.

[36] C. W. Tien, T. Y. Huang, C. W. Tien, T. C. Huang and S. Y. Kuo, "KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches," in Engineering Reports: Open Access, vol. 1, no. 5, 2019. DOI: 10.1002/eng2.12080.

[37] H. Hamzeh, S. Meacham and K. Khan, "A new approach to calculate resource limits with fairness in Kubernetes," in 2019 First International Conference on Digital Data Processing (DDP), 2019. Doi: 10.1145/3366615.3368356

[38] S. Suneja, A. Kanso and C. Isci, "Can container fusion be securely achieved?" in Proceedings of the 5th International Workshop on Container Technologies and Container Clouds, 2019, doi: 10.1145/3366615.3368356.

[39] B. Chun, J. Ha, S. Oh, H. Cho and M. Jeong, "Kubernetes Enhancement for 5G NFV Infrastructure" in 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, doi: 10.1109/ICTC46691.2019.8939817.

[40] A. Yeboah-Ofori, A. Jafar, T. Abisogun, I. Hilton, W. Oseni and A. Musa, "Data security and governance in multi-cloud computing environment" in 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud),pp. 215–222, 2024. doi: 10.1109/FiCloud62933.2024.00040.

[41] D. Soldani, P. Nahi, H. Bour, S. Jafarizadeh, M. F. Soliman, L. Di Giovanna, F. Monaco, G. Ognibene and F. Risso, "EBPF: A new approach to cloud-native observability, networking and security for current (5G) and future mobile networks (6G and beyond) " in IEEE Access: Practical Innovations, Open Solutions, vol. 11, pp. 57174–57202, 2023, doi: 10.1109/access.2023.3281480.

[42] A. Blaise and F. Rebecchi, "Stay at the Helm: secure Kubernetes deployments via graph generation and attack reconstruction," un 2022 IEEE 15th International Conference on Cloud Computing (CLOUD), 2022, doi: 10.1109/CLOUD55607.2022.00022.

[43] G. Budigiri, C. Baumann, J. T. Muhlberg, E. Truyen and W. Joosen, "Network policies in Kubernetes: Performance evaluation and security analysis," un 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2021, doi: 10.1109/EuCNC/6GSummit51104.2021.9482526.

[44] M. Ul Haque, M. M. Kholoosi and M. A. Babar, "KGSecConfig: A knowledge graph based approach for secured container orchestrator configuration," in 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 2022, doi: 10.1109/SANER53432.2022.00057.

[45] S. Lee and J. Nam, "Kunerva: Automated network policy discovery framework for containers" in IEEE Access: Practical Innovations, Open Solutions, vol. 11, pp. 95616–95631, 2023, doi: 10.1109/ACCESS.2023.3310281..

[46] J. M. Parra-Ullauri, L. F. Gonzalez, A. Bravalheri, R. Hussain, X. Vasilakos, I. Vidal, F. Valera, R. Nejabati, and D. Simeonidou, "Privacy preservation in Kubernetes-based federated learning: A networking approach," in IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–7, 2023, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225925.

[47] F. Hussain, W. Li, B. Noye, S. Sharieh and A. Ferworn, "Intelligent Service Mesh Framework for API Security and Management," in 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2019, doi: 10.1109/IEMCON.2019.8936216.

[48] J. Santos, E. Truyen, C. Baumann, F. De Turck, G. Budigiri and W. Joosen, "Towards intent-based scheduling for performance and security in edge-to-cloud networks," in 2024 27th Conference on Innovation in Clouds, Internet and Networks (ICIN), pp. 222–227, 2024, doi: 10.1109/ICIN60470.2024.10494432.

[49] R. R. Karn, P. Kudva, H. Huang, S. Suneja and I. M. Elfadel, "Cryptomining detection in container clouds using system calls and explainable machine learning," in IEEE Transactions on Parallel and Distributed Systems: A Publication of the IEEE Computer Society, vol. 32, no. 3, pp. 674–691, 2021, doi: 10.1109/tpds.2020.3029088.