Revista Científica de FAREM-Estelí
Medio ambiente, tecnología y desarrollo humano
Año 12 | Núm. 45 | Enero-marzo, 20223
ISSN: 2305-5790
https://rcientificaesteli.unan.edu.ni
DOI: https://doi.org/10.5377/farem.v12i45.16045

Principales riesgos de seguridad en computación móvil en la nube: una revisión de la literatura

Key security risks in mobile cloud computing: a literature review

Alberto Mendoza de los Santos
Universidad Nacional de Trujillo, Perú
https://orcid.org/0000-0002-0469-915X
amendozad@unitru.edu.pe

Jairo Aldair Ríos Reyes
Universidad Nacional de Trujillo, Perú
https://orcid.org/0000-0003-2865-6688
jariosr@unitru.edu.pe

Renzo Yampier Vásquez Chiclayo
Universidad Nacional de Trujillo, Perú
https://orcid.org/0000-0003-3388-4343
ryvasquez@unitru.edu.pe

Recibido
19/12/2022

Aceptado
27/03/2023

RESUMEN

La computación móvil en la nube está expandiéndose entre los usuarios de dispositivos móvil, brindando una plataforma para sus servicios dentro de estos dispositivos. El presente documento expone los principales riesgos de seguridad que existen en la computación móvil en la nube, desarrollando y describiendo lo siguiente: seguridad de los datos, seguridad de dispositivos, seguridad en la red móvil y seguridad en la nube, determinantes de robo de información y la vulnerabilidad de autenticación; se presentan los principales riesgos a los cuales se enfrentan la computación móvil en la nube, sin embargo existen muchas más vulnerabilidades y se brinda para la investigación de futuros lectores.

PALABRAS CLAVE

Mobile Cloud Computing; seguridad; riesgos; dispositivos móviles.

ABSTRACT

Mobile cloud computing is expanding among mobile device users, providing a platform for their services within these devices. This paper exposes the main security risks that exist in mobile cloud computing, developing and describing the following: data security, device security, mobile network security and cloud security, determinants of information theft and authentication vulnerability; the main risks faced by mobile cloud computing are presented, however many more vulnerabilities exist and are provided for future readers' research.

KEYWORDS

Mobile Cloud Computing; security; risks; mobile devices.

INTRODUCCIÓN

Para que podamos entender el significado de computación móvil en la nube (MCC), debemos tener claros los conceptos de computación en la nube (CC). La computación en la nube emerge como una tecnología la cual brinda funciones y medios informáticos a sus usuarios mediante la red pública la cual se especifica en la red. Sus usuarios usan aplicaciones, procesamiento de datos, etc. y la CC facilita su uso, ofreciendo nuevos rendimientos como, flexibilidad, eficiencia, etc.

Una vez explicada y entendida lo que es Cloud Computing, la computación móvil en la nube (MCC) ofrece diferentes servicios mediante la red portátil, es decir el manejo de la computación en la nube incorporándose con dispositivos portátiles (Muhseen, S. Abdul. S., & Elameer, A. S. ,2018, November 1).

En los últimos años, los dispositivos móviles que cuentan con múltiples funcionalidades y dentro de ello el almacenamiento de datos se está volviendo precario y poco utilizado por los usuarios, puesto que estos están siendo reemplazados por la computación móvil en la nube, pudiendo realizar el almacenamiento en servidores que rompen las restricciones de capacidad. Sin embargo, el uso de estos servidores en la nube ha ocasionado muchos retos para la seguridad y privacidad de datos puesto que la información de los usuarios sale de la protección del dispositivo y entran en la protección de la nube la cual debe brindar la confianza y resguardo necesario enfrentándose a ataques al dispositivo móvil, a la red y a la misma computación en la nube (Ikram, A. A., Rehman Javed, A., Rizwan, M., Abid, R., Crichigno, J., & Srivastava, G. ,2021).

El artículo de revisión restante está estructurado de la siguiente manera: la Sección II describe la metodología de investigación, dentro de ello redactamos el tipo de estudio donde planteamos la pregunta de investigación además los fundamentos y procesos de recolección de información, así como los criterios de exclusión e inclusión.

MATERIALES Y MÉTODOS

Tipo de Estudio

Se realizó una revisión sistemática de la literatura eligiendo a la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) (Page M, etc.,2021) como base. Durante el proceso metodológico logramos establecer la siguiente pregunta de investigación: ¿Cuáles son los principales riesgos de seguridad en la computación móvil en la nube?

Fundamentación de la metodología

La revisión sistemática conlleva a la acción de evaluar e interpretar toda la investigación disponible, de carácter importante en una interrogante de investigación particular o del área de interés (Manterola C. ,2013).

También, se hace una serie de investigaciones tanto en aspectos cuantitativos como cualitativos, con el fin de resumir esta información para el tema de interés.

En base a las definiciones que se mostraron, se puede observar la importancia de sintetizar la información, resaltando lo más relevante ante el efecto de la multiplicidad de investigaciones científicas que se dan en el paso del tiempo, para un resultado práctico en donde se logra identificar y evaluar diversos estudios de la misma área, pero con un objetivo en común, tomando en cuenta los sesgos de duplicidad y selección de los trabajos. En el presente, resulta complejo obtener conocimiento de la gran cantidad y/o exceso de información que hoy en día se publica.

Es por ello que la estrategia es necesaria para las interrogantes puntuales, con el fin de proveer una síntesis racional de la investigación básica.

El grupo MINCIR (Manterola C. ,2013), menciona que estas estrategias limitan los sesgos y errores aleatorios, debido a la ardua búsqueda de los artículos más relevantes, criterios reproducibles y explícitos de selección, además de la síntesis e interpretación de los resultados obtenidos; todo esto, gracias a la revisión sistemática de forma "objetiva, rigurosa y meticulosa", compactando la evidencia que se logra generar con el uso de las herramientas metodológicas y matemáticas para obtener la recolección de los datos en base a estudios primarios, pero rescatando cada efecto individual de los estudios que se obtuvieron.

Proceso de recolección de Información

El criterio de búsqueda se realizó utilizando como descriptores los siguientes términos en relación a la pregunta de investigación: "mobile security", "cloud computing", "mobile cloud computing". Para mejorar la búsqueda y poder clarificar las consultas, se diseñó la combinación de los términos antes mencionados y se agregó los operadores booleanos: [("mobile security") AND ("cloud computing") OR ("mobile cloud computing")]. De igual forma, se estableció como base de datos a SCOPUS y IEEE.

Las consultas de búsqueda específicas se detallarán a continuación:

Scopus:
(TITLE (mobile AND security) AND ABS (cloud AND computing) OR ABS (mobile AND cloud AND computing)) AND (LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE, "cr") OR LIMIT-TO (DOCTYPE, "re")) AND (LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR , 2020) OR

LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018))
IEEE:
("Document Title": mobile security) AND ("Abstract": cloud computing) AND ("Abstract": mobile cloud computing)

Tabla 1. *Distribución de artículos por base de datos*

Términos de búsqueda	Bases de datos	
	Scopus	IEEE
"mobile security", "cloud computing", "mobile cloud computing"	88	77
TOTAL	88	77

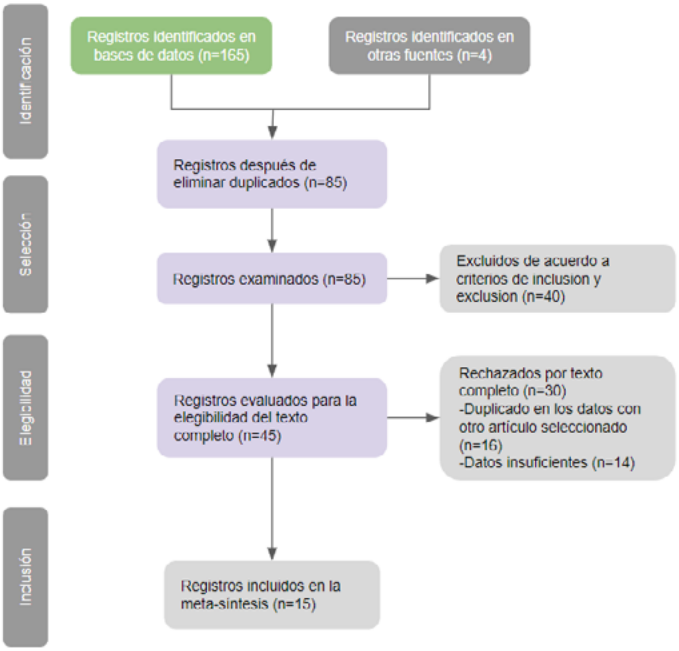
Criterios de Inclusión y Exclusión

Para el desarrollo del estudio, se obtuvieron artículos originales publicados en bases de datos científicas en inglés y español, en un margen de 5 años comprendido del 2018 a 2022. Estos artículos desarrollan los riesgos de seguridad que se dan en la computación móvil en la nube.

Como criterio de exclusión se determinó que deben ir fuera aquellos artículos que abordan la temática sobre redes 5G, computación perimetral y otros que no tengan relación directa con la seguridad en la computación móvil en la nube.

La planificación de la búsqueda y recopilación de información fue aplicada por dos revisores individualmente con su respectivo análisis, síntesis y conclusión en ambas partes mediante un mutuo acuerdo.

Figura 1. *Flujograma PRISMA. Elaboración propia.*



Fuente: Page M, etc. (2021).

RESULTADOS Y DISCUSION

Luego de realizar todo el proceso de filtro y exclusión del total de artículos se recopilaron estos, de los cuales se llevó a cabo la investigación sobre los principales riesgos en la seguridad de la Computación Móvil en la Nube; se realizó el listado de los riesgos presentes en cada artículo y se organizó por año de publicación como se presenta en la tabla 2.

Tabla 2. *Riesgos ordenados por año de publicación.*

Autores	Riesgo principal	Riesgo secundario
Vishal, Kaur, B., & Jangra, S. (2019).	• Interrupción de información • Administración y acreditación de accesos • Incautación de cuenta • Seguridad de dispositivo móvil • Incertidumbre en APIs	• Filtración de datos, confidencialidad. • Sistema de verificación, caracteres débiles, agresión de inicio de sesión. • Pérdida de contraseñas y acreditación, Phishing. • Claves secretas, flujo de actividad maliciosa. • Seguridad de organizaciones en la nube.
Muhseen, S. A. S., & Elameer, A. S. (2019).	• Terminal móvil • Seguridad de la red móvil • Nube móvil	• Malware, vulnerabilidades de software. • Fuga de información o ataque malicioso. • Confiabilidad de la plataforma, protección de datos.
Elzein, I. A., & Kurdi, M. (2019).	• Denegación de servicio • Autenticación	• Ataque DoS, inaccesibilidad del servicio. • Cifrado de información, phishing.
Hashim, A. S., & Awadh, W. A. (2018).	• Seguridad de datos • Conexión inalámbrica • Autenticación	• Almacenamiento de datos, confidencialidad e integridad. • Transferencia de datos • Acceso ilegal, suplantación de identidad.
Suo, H., Liu, Z., Wan, J., & Zhou, K. (2013).	• Servidor en la nube • Acceso no aprobado • Intercambio de datos	• Pérdida de información • Cálculo del cifrado • Almacenamiento de datos

Autores	Riesgo principal	Riesgo secundario
Ogwara, N. O., Petrova, K., & Yang, M. L. B. (2019).	• Seguridad de datos • Seguridad de la nube • Acceso no autorizado	• Datos del usuario, confidencialidad. • Interconexión de nubes, nodos de consumo. • Extracción información confidencial, IDS(Sistema de detección de intrusiones).
Neware, R., Ulabhaje, K., Karemore, G., Lokhande, H., & Dandige, V. (2020).	• Seguridad de datos • Seguridad de virtualización • Seguridad en descargas • Seguridad de aplicaciones en la nube • Seguridad de dispositivos móvil	• Violación y perdida de datos • Almacenamiento de datos • Acceso no autorizado, ataque root. • Obstrucción del dispositivo móvil, descarga maliciosa. • Software malicioso, malware. • Robo de dispositivo, ataque DoS.
Qayyum, R., & Ejaz, H. (2020).	• Pérdida de confidencialidad • Seguridad de datos	• Control de acceso • Intercambio de datos en la nube. • Almacenamiento de datos.
Fellah, H., Mezioud, C., & Batouche, M. C. (2020).	• Seguridad de dispositivos móviles • Seguridad de red móvil • Seguridad de la nube	• Malware, vulnerabilidad de software. • Redes inalámbricas, servicio de telefonía, dirección IP. • APIs inseguras, vulnerabilidades del sistema, insiders maliciosos, pérdida de datos.
Hanamantraya, & Subhajini, A. C. (2020).	• Componentes de identificación • Intercambio de datos	• Cifrado de la información, brechas de seguridad. • Administración de claves, robo de información.
Merdassi, I., Ghazel, C., & Saidane, L. (2020).	• Seguridad de la aplicación móvil • Seguridad de la red móvil • Privacidad	• Servicios de seguridad en la nube, detección de programas locales. • Código malicioso, aplicaciones “riskware”. • Información personal, geolocalización.

Autores	Riesgo principal	Riesgo secundario
Jena, S. R., Yadav, A. K., Patel, S., & Saibaba, C. H. M. H. (2021).	• Seguridad de Red móvil • Seguridad de la nube	• Encriptación de información, seguridad del sistema. • Métodos de autenticación, privacidad de datos.

La computación móvil y la computación en la nube se combinan para formar la computación móvil en la nube (MCC) a fin de brindar servicios de nube a los usuarios móviles, como autoservicio bajo demanda, servicios medidos de agrupación de recursos, flexibilidad, amplio acceso a la red (Muhseen, S. A. S., & Elameer, A. S. ,2019). MCC utiliza tecnología de comunicación inalámbrica para comunicarse entre el móvil y la nube. Esto presenta múltiples desafíos tales como recursos limitados en dispositivos móviles, problemas de estabilidad debido a la limitación de la red inalámbrica, aumento de costos de acceso a la red, problemas de seguridad y privacidad, ancho de banda, etc.

En la actualidad, los dispositivos móviles siguen sufriendo de una amenaza en la seguridad y además de la preocupación del usuario. Cuando este dispositivo es extraviado o robado, los datos personales se verán comprometidos.

El principal desafío se relaciona con las características especiales de redes inalámbricas y dispositivos móviles (Elzein, I. A., & Kurdi, M. ,2019). El tema de la seguridad en la Computación móvil en la nube es fundamental para la transmisión de los datos, y estos problemas de seguridad son una obstrucción para su rápido crecimiento, problemas como la falta de confiabilidad, la no confidencialidad, etc.

Reglas de seguridad que debe tener la computación móvil en la nube

- **Confidencialidad:** La confidencialidad es un requisito fundamental debido a que los datos de los usuarios se procesan mediante la red pública y se almacenan en servidores públicos. Por lo cual, el acceso de la información debe estar controlado y solo ser accedida por el usuario que se encuentra autorizado, esto para salvaguardar la información y lo cual es un gran desafío para los proveedores de servicios móviles en la nube (Ogwara, N. O., Petrova, K., & Yang, M. L. B. ,2019).
- **Disponibilidad:** Significa que el servicio debe estar disponible para los usuarios las 24 horas del día, los 7 días de la semana cada que lo necesiten. Los proveedores deben prevenir ataques y asegurar la continuidad del servicio (Merdassi, I., Ghazel, C., & Saidane, L. ,2020).
- **Integridad:** En la integridad se debe incorporar la información que el usuario mantiene en la nube mediante un dispositivo móvil. Se debe asegurar que los datos o información sean dirigidos o almacenados de manera completa, sin que se haya producido alguna alteración de pérdida de estos de manera accidental o intencional (Qayyum, R., & Ejaz, H. ,2020).

- **Autenticación y Control de Acceso:** El problema principal cuando se requiere acceder a los datos almacenados en la nube es garantizar que el usuario acceda a sus datos y no permitir el acceso no autorizado de externos mediante varios instrumentos de verificación, los cuales pueden ser: identificador de inicio de sesión, contraseñas, PINs o cualquier otro método de autenticación (Jena, S. R., Yadav, A. K., Patel, S., & Saibaba, C. H. M. H. ,2021). Permitir el acceso a recursos limitados para autenticar a los usuarios del sistema al momento de realizar alguna tarea se denomina control de acceso, en donde se pueden controlar acciones como: leer, escribir, actualizar, borrar datos, etc. (Suo, H., Liu, Z., Wan, J., & Zhou, K. ,2013).
- **Privacidad:** La privacidad es la seguridad de los datos personales del usuario mientras se realiza la comunicación con la nube, lograda mediante la confidencialidad, la integridad y la autenticación (Neware, R., Ulabhaje, K., Karemore, G., Lokhande, H., & Dandige, V., 2020).

Después de analizar los riesgos más frecuentes en cada uno de los artículos, se llegó a la elaboración de una tabla para agrupar estos datos y poder clasificarlos mediante un tipo de riesgo en la seguridad de MCC como se muestra en la tabla 3.

Tabla 3. *Tipos de riesgos a la seguridad de MCC.*

Código	Descripción
R1	Infiltración de datos: se compromete la confidencialidad e integridad de los datos
R2	Deficiencia en gestión de identidad, credenciales y acceso: permite el acceso no autorizado a los datos
R3	APIs (Interfaces de programación de aplicaciones) inseguras: lleva a filtraciones de datos
R4	Vulnerabilidad en dispositivos móviles y aplicaciones: ataques al entorno de MCC
R5	Robo de cuenta: pérdida del dispositivo móvil o el uso no autorizado de las credenciales para un acceso ilegal a MCC
R6	Insiders maliciosos: un usuario de la organización lanza ataques intencionalmente
R7	Amenazas persistentes avanzadas (APT): ataque intencional hacia un objetivo específico
R8	Pérdida de datos: luego de un ataque, supresión accidental, daño en el almacenamiento, desastre natural y error en la transmisión de datos.
R9	Clon móvil: seguridad de la virtualización en Mobile Cloud Computing
R10	Denegación de servicio (DoS): restringir el acceso a la nube de los usuarios legítimos de MCC.

Principales problemas de la seguridad en la computación móvil en la nube.

La unión de la MC y la computación en la nube forman lo que es la MCC, por ende, los problemas de seguridad de la MCC se heredan de los problemas de seguridad de MC y Cloud Computing, teniendo una alta gama de problemas de seguridad que lo vuelve altamente vulnerable.

1. Seguridad de los datos

En la computación móvil en la nube (MCC), los datos de los usuarios están disponibles y almacenados en la nube, y el procesamiento de estos también se realiza en la Infraestructura como Servicio (IaaS) de la nube.

Muchos de los ataques que se ejecutan en la MCC son a cerca de la pérdida de datos, violación de datos, recuperación de datos dañados, datos locales, corrección de datos, etc. (Tal vez se pueda realizar en una tabla)

En la pérdida de datos, los datos del usuario se destruyen mientras se realiza cualquier tarea computacional; por ejemplo, al transmitir datos a través de una red pública. En las violaciones de datos, una persona no autorizada accede a los datos de un usuario interceptados en la nube o los obtiene mediante cualquier actividad no deseada. En la recuperación de datos dañados, un usuario debe obtener sus propios datos válidos mientras se recupera debido a daños en el sistema o dispositivo móvil.

La nube almacena los datos en cualquier centro de datos; por lo que la ubicación de esos datos no es conocida por nadie. Entonces, el desafío es que el usuario sepa dónde se almacenan sus datos importantes. La gestión de datos se realiza en las instalaciones de los proveedores de servicios y deben mantener la confidencialidad y la integridad (Neware, R., Ulabhaje, K., Karemore, G., Lokhande, H., & Dandige, V.,2020).

2. Seguridad de los dispositivos móviles

Los dispositivos móviles almacenan información personal ya sean fotos, contactos, videos, etc. así mismo información confidencial como claves de usuario e información de tarjetas de crédito o débito y esto ocasiona un atractivo por parte de los atacantes, además, debido a las limitaciones que encontramos en los recursos y sistemas de seguridad ya que no se pueden instalar certeras aplicaciones contra estas amenazas Fellah, H., Mezioud, C., & Batouche, M. C. (2020).

A continuación, detallaremos los riesgos de los dispositivos móviles:

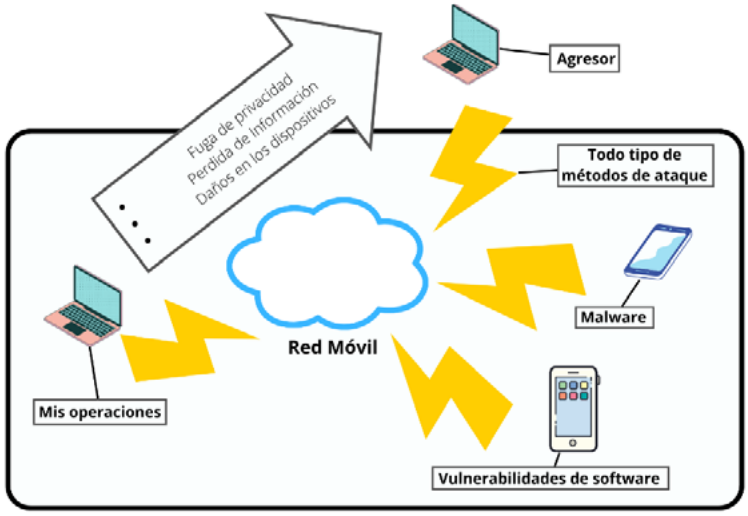
A. Malware.

El Malware en los dispositivos móviles inicia por alguna descarga de algún programa útil, pero de dudosa procedencia, teniendo dentro un virus o troyano y dañando tu dispositivo sin que el usuario se diera cuenta. Esto con la finalidad del robo de información o pérdidas económicas (Suo, H., Liu, Z., Wan, J., & Zhou, K., 2013). Otras maneras de propagación son las redes 4G, Bluetooth o MMS.

B. Vulnerabilidades de Software

1. **Software de la aplicación:** Estas vulnerabilidades son las más encontradas ya que los ataques pueden asediar el teléfono móvil por un error de software de la aplicación puesto que este es poco riguroso Fellah, H., Mezioud, C., & Batouche, M. C. (2020).
2. **Sistema Operativo:** El sistema operativo administra y controla el hardware y software, este último es tan complejo que arroja errores de configuración. Los atacantes aprovechan estos errores y arremeten contra el teléfono móvil vulnerando su seguridad Fellah, H., Mezioud, C., & Batouche, M. C. (2020). Un ejemplo de esto es el Android 2.3 Gingerbread, el cual en la actualidad además de ser precario ya no es compatible con Google y fue considerado uno de los sistemas operativos móviles con más ataques de malware.
3. **Otros riesgos de dispositivos móviles:** Así como vimos que los riesgos o problemas pueden ser por parte del software o hardware del mismo teléfono móvil, los riesgos y problemas pueden provenir de los mismos usuarios, los cuales algunos carecen de conciencia y capacitación y esto conlleva a realizar un mal uso de sus dispositivos móviles. Esto también podría ocasionar posible filtración de datos y daños en los dispositivos. Por tanto, sigue siendo necesario y fundamental registrar y prever comportamientos anómalos de los usuarios.

Figura 2. *Problemas de seguridad de dispositivos móviles.*



Fuente: Elameer, A. S. & Muhseen, S. A. S. (2019).

3. Seguridad en redes móviles

En la actualidad los usuarios acceden a la red en todo momento vía algún servicio de internet como red 4G, Wi-Fi y Bluetooth. En este acceso a la red el usuario el tráfico de datos o información en la red es alto, dentro de esa información se encuentra la información confidencial, ya sean número de tarjetas de crédito o débito, usuarios y contraseñas, etc.

Aumenta el riesgo mediante esta transferencia de información desde la nube al dispositivo móvil y viceversa. La conexión a redes de internet por medio de conexión Wi-Fi gratuita que se encuentran en cafeterías, restaurantes, aeropuertos, etc. pueden facilitar a los atacantes informáticos los medios para robar información personal u otro ataque malicioso en contra del usuario.

Más actualmente con el avance de la tecnología se realizan transferencias interbancarias desde los dispositivos móviles es por eso que siempre se debe ser cuidadoso de la conexión de acceso a internet.

4. Seguridad en la nube

La computación en la nube forma parte actualmente del almacenamiento de datos, aplicaciones y cargas de trabajo es por eso que la seguridad de la nube tiene grandes desafíos por la gran cantidad de amenazas como la confidencialidad, pérdida de datos, pérdida de datos, etc.

a. Infiltración de datos

El usuario que registra su información en la nube debe tener toda la certeza de que su información no será difundida y que el proceso de traslado de datos sea el más completo y seguro ya que los atacantes podrían acceder fácilmente a ella si se cuenta con vulnerabilidades en la nube (Neware, R., Ulabhaje, K., Karemore, G., Lokhande, H., & Dandige, V., 2020).

b. Deficiencia en gestión de identidad, credenciales y acceso

El acceso a la información debe estar restringido para algunos usuarios que cuentan con una autenticación y el acceso con otra autenticación debe ser restringida completamente (Muhseen, S. A. S., & Elameer, A. S., 2019).

c. Interfaces inseguras e interfaces de programación de aplicaciones (API)

El proveedor que da el acceso a la nube cuenta con un conjunto de interfaces de usuario (UI) o APIs de software en donde los clientes usan para organizar e interactuar con los servicios de la nube. Todas las acciones se realizan en estas interfaces y la su seguridad depende de la seguridad de las APIs (Vishal, Kaur, B., & Jangra, S.,2019).

d. Sistemas vulnerables

Estas vulnerabilidades son netamente en los programas que se desarrollaron para cierto proceso, donde los atacantes pueden detectar e infiltrarse con la finalidad de robar datos, apropiarse del sistema o interrumpir operaciones que realiza el usuario normalmente.

e. Secuestro de cuentas

A raíz del riesgo anterior, si los atacantes logran acceder al sistema mediante la obtención de las credenciales de un usuario puede observar actividades y transacciones confidenciales, así como información calificada y redirigir al usuario a sitios ilegítimos. Con esas credenciales los atacantes pueden acceder a áreas críticas de los servicios de computación en la nube, lo que compromete la confidencialidad integridad y la disponibilidad de esos servicios.

f. Incidentes maliciosos

Dentro de una organización podría haber alguna persona con malas intenciones que tenga el rol de administrador de usuario del sistema y este pueda acceder a información sumamente confidencial.

g. Pérdida de datos

Sabemos que la seguridad de los datos es la principal preocupación de la computación en la nube, además que los usuarios brindan información confidencial a través de la red. La pérdida de datos puede ocasionar por distintos motivos. Puede ser algo accidental por parte del proveedor de servicios en la nube o algo físico como un incendio, inundación o terremoto, es por esto que se deben tomar medidas preventivas por parte del proveedor o el consumidor, además se deben realizar copias de seguridad de los datos.

5. Seguridad de la virtualización

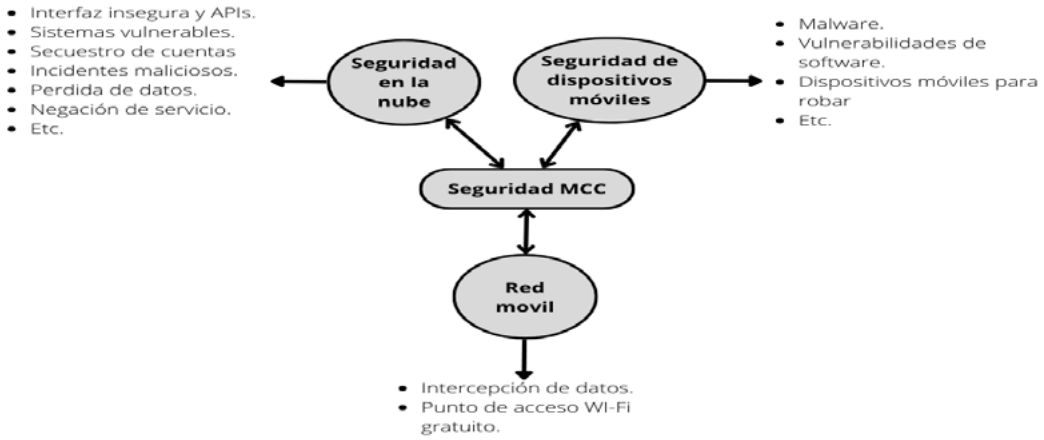
Los servicios en la nube se proporcionan a los usuarios móviles mediante la virtualización. Una máquina virtual de móvil se vuelve a instalar en la nube, lo que se denomina clon móvil, y esta máquina virtual basada en la nube hace todo el procesamiento. La principal ventaja de usar una máquina virtual es que crea instancias de varias máquinas y esto se logra a través del hipervisor (Merdassi, I., Ghazel, C., & Saidane, L.,2020).

Pero los desafíos para la máquina virtual utilizada en la computación en la nube son el acceso no autorizado a la máquina principal a través de la máquina virtual, el ataque raíz, el ataque de VM a VM, la comunicación en la virtualización y la confidencialidad de los datos mientras se procesan a través del hipervisor.

6. Denegación del Servicio (DoS)

Los ataques DoS están diseñados para evitar que los usuarios de un servicio puedan acceder a sus datos o aplicaciones. Al obligar al servicio en la nube objetivo a consumir cantidades excesivas de recursos finitos del sistema, como la potencia del procesador, la memoria, el espacio en disco o el ancho de banda de la red, los atacantes pueden provocar una ralentización del sistema y dejar a todos los usuarios legítimos del servicio sin acceso a los servicios.

Figura 3. *Problemas de seguridad en MCC.*



Fuente: Batouche, M. C., Fellah, H. & Mezioud, C. (2020).

Los resultados que se muestran en el presente artículo, responden a nuestra pregunta de investigación, mencionando y describiendo cuales son los principales riesgos de seguridad de la computación en la nube sin embargo existen muchos desafíos relacionados con la seguridad y privacidad que aún están en investigación y a esperas de su resolución. Por último, la intención del artículo solo es informar de los principales riesgos que se han logrado encontrar en demás artículos, pero no, brindar una solución ante cada uno de estos, por eso se recomienda a los lectores que tomen como referencia este artículo para que aborden más en el tema y puedan formular soluciones ante estos riesgos.

CONCLUSIONES

En este artículo se presenta una descripción de los riesgos de seguridad que afronta la MCC los cuales son divididos en tres aspectos: dispositivo móvil, computación en la nube y red móvil; se describieron cada uno de estos riesgos, de manera clara y precisa.

En el desarrollo de este artículo se describió que la MCC cuenta con múltiples riesgos y vulnerabilidades de seguridad a causa de la abundante información que viaja por la red y los atacantes quieren apoderarse. Finalmente podemos observar en la tabla 2 un resumen de los riesgos de la MCC. Esperamos que

este documento sirva para que otros lectores puedan comparar, analizar y dirigir futuras investigaciones además que sea beneficioso para dar una pista sobre el camino a seguir y permitir una integración masiva de la computación móvil y la computación en la nube.

REFERENCIAS BIBLIOGRAFICAS

Elameer, A. S. & Muhseen, S. Abdul. S. (2018, November 1). A Review in Security Issues and Challenges on Mobile Cloud Computing (MCC). IEEE Xplore. https://doi.org/10.1109/AiCIS.2018.00035

Abid, R., Crichigno, J., Ikram, A. A., Rehman Javed, A., Rizwan, M., & Srivastava, G. (2021). Mobile Cloud Computing Framework for Securing Data. 2021 44th International Conference on Telecommunications and Signal Processing (TSP). https://doi.org/10.1109/tsp52935.2021.9522673

Page M, etc. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. doi: 10.1136/bmj.n71

Manterola C. (2013). Revisiones sistemáticas de la literatura. Qué se debe saber acerca de ellas. doi: 10.1016/j.ciresp.2011.07.009

Jangra, S. & Vishal, Kaur, B. (2019). Assessment of different security issues, threats with their detection and prevention security models in mobile cloud computing (MCC) doi:10.1007/978-981-13-3143-5_27

Elameer, A. S. & Muhseen, S. A. S. (2019). A review in security issues and challenges on mobile cloud computing (MCC). Paper presented at the Proceedings - 2018 1st Annual International Conference on Information and Sciences, AiCIS 2018, 133-139. doi:10.1109/AiCIS.2018.00035

Elzein, I. A., & Kurdi, M. (2019). Analyzing the challenges of security threats and personal information in mobile cloud computing infrastructure. Paper presented at the Proceeding of 2019 International Conference on Digitization: Landscaping Artificial Intelligence, ICD 2019, 202-206. doi:10.1109/ICD47981.2019.9105711

Awadh, W. A. & Hashim, A. S. (2018). Investigation of security and privacy methods for public mobile cloud computing. Journal of Engineering and Applied Sciences, 13(12), 4396-4402. doi:10.3923/jeasci.2018.4396.4402

Liu, Z., Suo, H., Wan, J., & Zhou, K. (2013). Security and privacy in mobile cloud computing. Paper presented at the 2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013, 655-659. doi:10.1109/IWCMC.2013.6583635

Ogwara, N. O., Petrova, K., & Yang, M. L. B. (2019). Data Security Frameworks for Mobile Cloud Computing: A Comprehensive Review of the Literature. 2019 29th International Telecommunication Networks and Applications Conference (ITNAC). https://doi.org/10.1109/itnac46935.2019.9078007

Dandige, V., Karemore, G., Lokhande, H., Neware, R. & Ulabhaje, K. (2020). Survey on security issues in mobile cloud computing and preventive measures doi:10.1007/978-981-13-9680-9_6

Batouche, M. C., Fellah, H. & Mezioud, C. (2020). Mobile cloud computing:

Architecture, advantages and security issues. Paper presented at the ACM International Conference Proceeding Series, doi:10.1145/3386723.3387880

Ejaz, H. & Qayyum, R. (2020). Data security in mobile cloud computing: A state of the art review. International Journal of Modern Education and Computer Science, 12(2), 30-35. doi:10.5815/ijmecs.2020.02.04

Ghazel, C., Merdassi, I. & Saidane, L. (2020). Surveying and analyzing security issues in mobile cloud computing. Paper presented at the 2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks, PEMWN 2020, doi:10.23919/PEMWN50727.2020.9293077

Hanamantraya, & Subhajini, A. C. (2020). Security of data in mobile cloud computing and its significance. International Journal of Scientific and Technology Research, 9(2), 289-294.

Jena, S. R., Patel, S., Saibaba, C. H. M. H & Yadav, A. K. (2021). Analysis on mobile cloud security and comparison of existing models. Indian Journal of Computer Science and Engineering, 12(3), 580-590. doi:10.21817/indjcse/2021/v12i3/211203065