Seguridad y protección de la Información en la Nube de Cómputo

Security and Protection of Information in the Cloud of Computation

Valeria Herrera Salazar[1]

1. Docente del Área de la Educación, el Arte y la Comunicación

*Autor para correspondencia: vherrera@unl.edu.ec

RECIBIDO: 14/04/2016

APROBADO: 16/11/2016

RESUMEN

La seguridad de los datos siempre ha sido una importante tecnología de información y comunicación. Los datos y la información en la nube o mejor conocido como "cloud computing" se vuelve más importante porque los datos están en diferentes lugares alrededor del mundo. La seguridad de los datos y la protección de la privacidad son dos factores principales de interés para el usuario al utilizar esta tecnología. Se han realizado muchas investigaciones sobre este tema en el ámbito académico, tecnológico, gubernamental, industrial y empresarial, siempre coincidiendo en que la seguridad de los datos y la protección de la privacidad son cada vez más importantes para el desarrollo futuro de esta importante y necesaria herramienta tecnológica. Este artículo discute diferentes estudios sobre cloud computing, con el fin de verificar diversas técnicas de seguridad, tanto de software como de hardware, para diseñar nuevos procedimientos y aumentar su fiabilidad.

Palabras clave: Cloud Computing; seguridad de datos; protección de la privacidad; información en la nube.

ABSTRACT

Data security has always been an important technology of information and communication issue. Data and information in the cloud or better known as "cloud computing" becomes more important because the data are in different places around the world. Data security and privacy protection are two main factors of interest for user when using this technology. There has been much research on this topic in academic, technological, government environment, industry and business fields, always agreeing that data security and privacy protection are increasingly important for the future development of this important and necessary technological tool. This article discusses different studies about cloud computing, in order to check various security techniques, both software and hardware, to designing new procedures and increasing its reliability

Keywords: Cloud Computing; Data security; Protection of privacy; Information in the cloud.

N°6, diciembre 2016
ISSN: 1390-9029
Revista EAC

INTRODUCCIÓN

Cloud Computing (CC), o computación en la nube, se ha concebido como el modelo a seguir en la próxima generación de las tecnologías de la información y comunicación (TIC's). CC se define como un medio ambiente en donde la información y los datos se encuentran en servidores centralizados para proporcionar diversos servicios al usuario a través de la red de Internet (Leavitt, 2009). La explicación del Instituto Nacional de Estándares y Tecnología (NIST), es que CC permite, convenientemente el acceso extendido a la red y a un conjunto compartido de recursos informáticos configurables, p. ej. Redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente guardados y liberados con un esfuerzo mínimo de gestión o interacción por parte del proveedor de servicios (Mell & Grance, 2010). De acuerdo con esta explicación, CC ofrece un cómodo acceso a la red a un conjunto compartido de recursos informáticos. El usuario dispondrá entonces de diferentes aplicaciones informáticas únicamente conectándose a la red desde cualquier lugar con acceso, y tener para sí plataformas, servicios de software, servidores virtuales, y toda la infraestructura necesaria para continuar con sus actividades como si estuviera en su propio hardware.

Una de las principales preocupaciones de CC es el manejo de los datos, tanto en redes públicas y privadas. Como CC se convierte en la plataforma principal, las preocupaciones relativas a la seguridad, almacenamiento y transferencia de datos han crecido en importancia. Para aumentar la preocupación relativa a esta tecnología, diversos países tienen políticas de gobierno para el acceso a los datos, por ejemplo, limitar que la información no salga de una frontera. En una encuesta realizada, se demostró que el 88% de los consumidores están preocupados por saber quién tiene acceso a sus datos, y aún más, que ni siquiera desean que sus datos se muevan fuera de las fronteras de su nación (Yu Shyang Tan et al., 2012).

En comparación con el modelo tradicional de las TIC's, CC tiene muchas ventajas potenciales. Pero desde la perspectiva de los consumidores, las preocupaciones de seguridad de CC siguen siendo un obstáculo importante para su adopción. De acuerdo con una encuesta de la *International Data Corporation* (IDC) en 2009, el 74 % de los gerentes en las industrias de telecomunicación creen que el reto principal para el uso de los servicios de CC son los problemas de seguridad. Otra encuesta indica que más del 70 % de los directores de tecnología creen que la principal razón para no utilizar los servicios de CC es que haya problemas de seguridad en los datos y privacidad (Deyan Chen & Hong Zhao, 2012).

ARQUITECTURA EN CLOUD COMPUTING

Según Wang, Wang, Ren, Lou, & Li, (2011), la arquitectura más representativa para CC es la que se puede mostrar en la fig. 1. Tres diferentes entidades de red se identifican en este modelo:

Cliente: Es una entidad que tiene los archivos o datos que serán almacenados en la nube, pueden ser de usuarios individuales u organizaciones.

Servidor de almacenamiento (Cloud Storage Server – CSS): Es una entidad que es administrada por el Proveedor de Servicios (Cloud Service Provider - CSP), debe tener el suficiente espacio de almacenamiento para resguardar los datos de los clientes.

Auditor externo (Third party auditor): Es una entidad, que cuenta con experiencia y capacidades que los clientes no tienen, evalua y exponer los riesgos de los servicios de almacenamiento en la nube cuando los clientes lo soliciten.

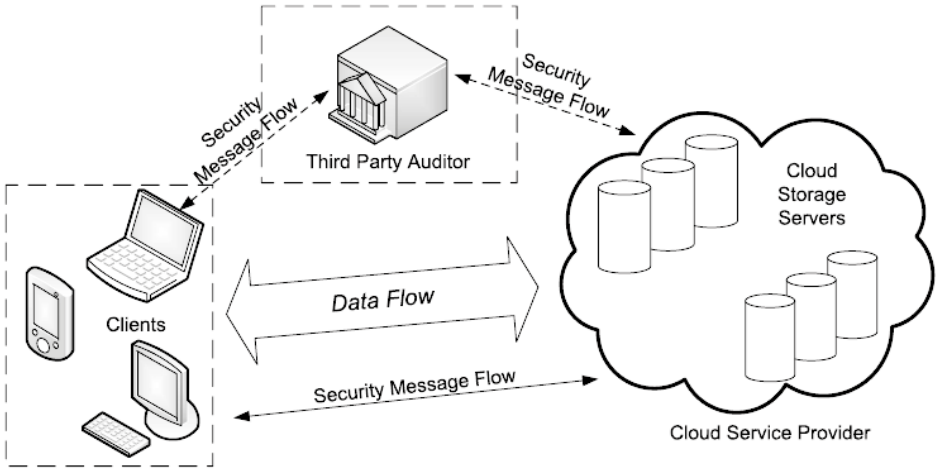

Fig 1. Arquitectura de almacenamiento en cloud computing.

En un estudio se indica que, en este esquema, el cliente puede solicitar periódicamente al servidor los archivos para asegurar la exactitud de la información, y los datos originales pueden ser recuperados mediante la interacción con el servidor (Shacham & Waters, 2013). En Kirkham et al., (2012) este esquema se podría complicar si el CSP no trata directamente con el interesado, sino que tiene contacto con un consumidor de servicios que podría ser cualquier otra organización.

La seguridad se puede concebir como la combinación de la confidencialidad, la integridad de los datos y la prevención frente a la divulgación, modificación, supresión y/o retención no autorizada de la información. Según las diferencias para el acceso a la nube, ésta puede dividirse en tres tipos: pública, privada e híbrida (Avizienis, Laprie, Randell, & Landwehr, 2004). La nube pública significa que los servicios de red están disponibles para todos, la nube privada se refiere específicamente a la nube en la que sólo los usuarios autorizados pueden acceder a los servicios del proveedor, y la nube híbrida es la mezcla de ambas. La mayoría de nubes públicas y privadas de los servicios en los CC existentes son proporcionados por grandes empresas de servicios tales como Google, Amazon e IBM.

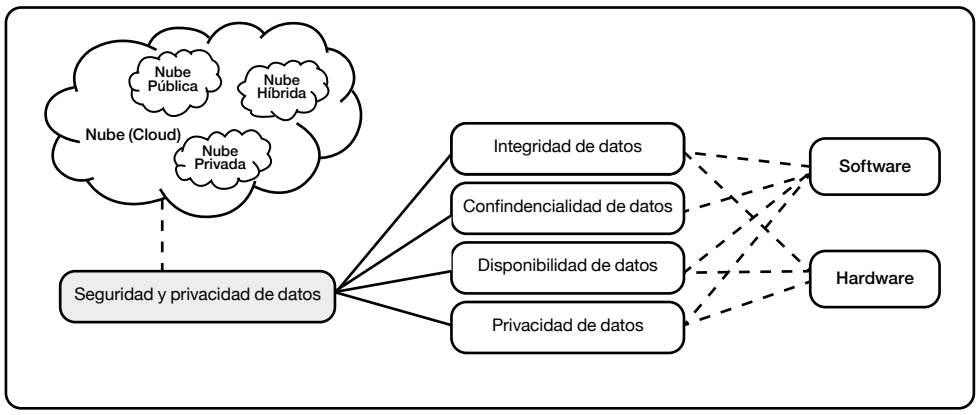

Fig 2. Organización de la seguridad y privacidad de los datos en CC.

N°6, diciembre 2016
ISSN: 1390-9029
Revista EAC

Como muestra la fig. 2, existen cuatro ámbitos esenciales en los que debe enfocarse la investigación en CC como son: seguridad de datos, incluyendo la integridad de datos, confidencialidad, disponibilidad y privacidad. Estudios sobre la seguridad de datos y la privacidad podrían ayudar a mejorar la confianza del usuario y a asegurar la disponibilidad de los datos en el cloud computing.

III. SEGURIDAD Y PROTECCIÓN DE DATOS

A. Seguridad de la información

Hay muchos problemas de seguridad asociados con CC y que pueden agruparse dentro de los siguientes temas: acceso de datos, condiciones de servicio, ubicación de los datos, recuperación de los datos, apoyo técnico y viabilidad a largo plazo. Según Hurst, (2011) en el año 2009 se evaluaron las prácticas de seguridad y privacidad de algunos de los principales proveedores de CC (Salesforce.com, Amazon, Google, y Microsoft) en tres aspectos principales: la seguridad y la privacidad, el cumplimiento, y las cuestiones legales/contractuales. Así mismo Cloud Security Alliance (CSA) invitó a los proveedores sin fines de lucro e individuos a discutir sobre prácticas actuales y futuras para mejorar la seguridad de la información en la red, identificando trece temas que preocupan sobre la seguridad de CC, derivados de los puntos anteriores. Subashini & Kavitha, (2011) hicieron una investigación de los problemas de seguridad de CC y de sus modelos tradicionales como es el SPI (Software, Plataform, Infraestrcuture) de la fig. 3, para dar un análisis detallado de cada problema de seguridad.

Bouayad, Blilat, El Houda Mejhed, & El Ghazi, (2012) exploraron los temas de seguridad en CC desde diferentes perspectivas, incluyendo los problemas de seguridad asociados con la arquitectura de los modelos SPI. Ellos creen que dos aspectos son esenciales para esta tecnología: confianza y auditoría. También señalan que en los modelos tradicionales existen problemas de seguridad en todos los aspectos de la infraestructura, incluyendo nivel de red, nivel de host y nivel de aplicación.

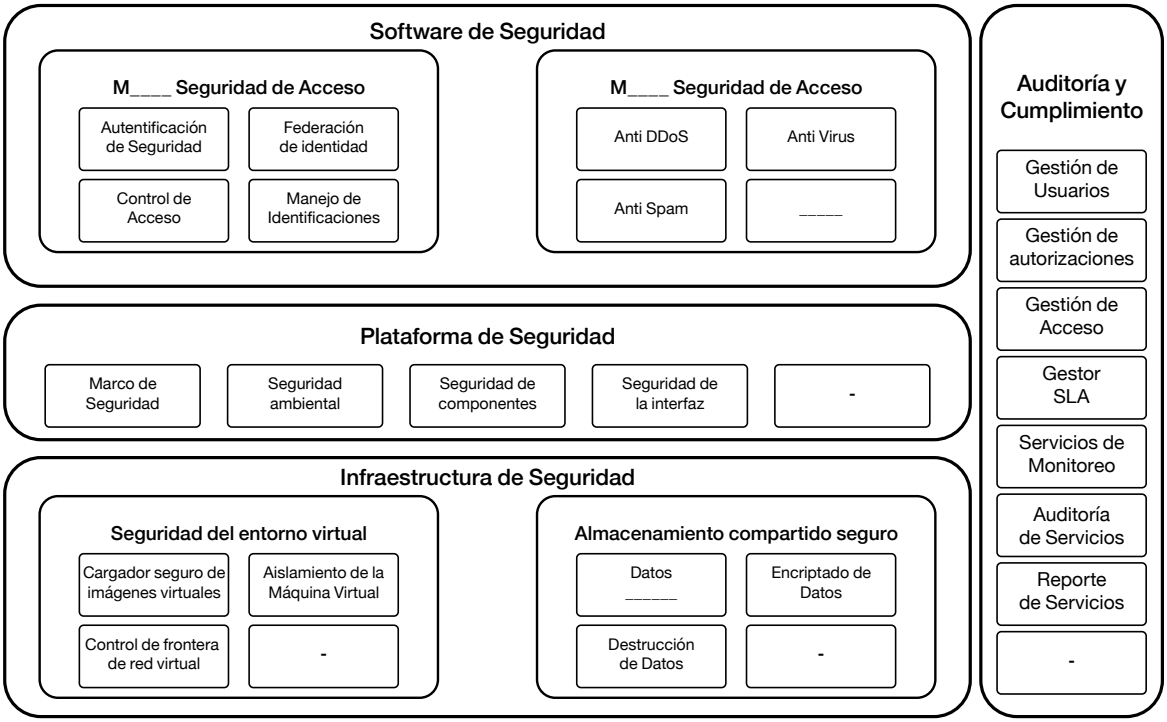

Fig 3. Modelo de seguridad SPI en cloud computing

B. Protección de la privacidad

Un estudio de la Asociación Internacional de Profesionales de la Privacidad (IAPP) informa que el 98% de las empresas tienen políticas de privacidad. A menudo las organizaciones tienen políticas internas adicionales a las reglas estatales sobre el manejo de la información, y también se acogen a las políticas exteriores en términos de informar a los titulares sobre el uso de su información (Karat, Karat, Brodie, & Feng, 2005).

La protección de la privacidad en la nube es similar a la protección de la privacidad de datos en general. También está involucrada en cada etapa del ciclo de vida de los datos. Pero a causa de la apertura y los "multi-usuarios" característico de CC, el contenido de la protección de la privacidad en la nube tiene sus particularidades. El concepto de privacidad es muy diferente en los distintos países, culturas o jurisdicciones. De acuerdo al Instituto Americano de Contadores Públicos Certificados (AICPA) la privacidad debe evitar "la recopilación, uso, retención y divulgación de información personal". En términos generales, la privacidad protege la manipulación y destrucción de datos personales (o identificación falsa). Por lo tanto, la identificación del usuario es la tarea primordial dentro de la protección de la privacidad (Deyan Chen & Hong Zhao, 2012).

Además de la función primordial del usuario, los CSP necesitan implementar controles internos, y un proceso de auditoría externa. El entorno de CC presenta nuevos desafíos desde una perspectiva de auditoría y cumplimiento, pero las soluciones existentes para la contratación externa y la auditoría se pueden aprovechar (Pearson & Benameur, 2010). Los negocios realizados con los datos que residen en la nube deben estar correctamente resguardados, con el fin de garantizar la integridad de los datos, debido a que el usuario confiará de forma transparente en las decisiones del CSP.

IV. SOLUCIONES ENCONTRADAS

IBM desarrolló un esquema de cifrado completamente homomórfico en junio de 2009. Este esquema permite que los datos sean procesados sin ser descifrados (IBM seguiridad.2010). La Organización para el Avance de Estándares de Información Estructurada (OASIS) y el Protocolo de Interoperabilidad y Administración de Claves (KMIP) está tratando de resolver este tipo de problemas. Sobre la integridad de los datos, debido al envío y recepción, las tasas de transferencia y error, así como el tiempo de descarga, los usuarios deben primero identificarse, y a medida que los datos son dinámicos, las soluciones tradicionales de integridad de datos ya no son adecuadas (Zeng, 2008). Wang et al., (2011) propusieron una forma matemática para verificar la integridad de los datos almacenados dinámicamente en la nube.

Gajanayake, Iannella, & Sahama, (2011) proponen un modelo para la protección de la privacidad e integridad basada en la auditoría de la información, lo que se conoce como information accountability (IA). Este procedimiento puede identificar a los usuarios que acceden a la información y los tipos de información que utilizan. Cuando se detecta el mal uso o uso inapropiado, IA define un conjunto de métodos para identificar a los usuarios responsables. Estas técnicas también son utilizadas por el Departamento de Defensa de los Estados Unidos (DoD).

Otra solución encontrada en un estudio es el seguimiento de datos. El uso de esta técnica es capaz de seguir y proteger los datos, y se hace en el momento que la información está a punto de ser trasladada a la nube. Cuando un usuario intenta copiar o eliminar uno o más archivos fuera de los límites de la nube, debe cumplir un registro de check-out a través de una interfaz web proporcionada (Yu Shyang Tan et al., 2012).

N°6, diciembre 2016
ISSN: 1390-9029
Revista EAC

En estos sistemas los archivos de datos se encapsulan junto con un programa de visualización, en un contenedor de aplicación directa. Esto funciona como un archivo *.zip autoextraíble donde una vez ejecutado, en lugar de archivar el contenido, la aplicación ejecuta el wiewer.exe que se encuentra dentro del contenedor. Una vez que los diversos archivos de datos y el programa se archivan, estos se encriptan para evitar que los usuarios puedan tener acceso. De esta manera, sólo el usuario tendrá acceso a la información, ya que sólo él tiene la clave, que es solicitada en el momento de crear el contenedor, para descifrar los datos encriptados.

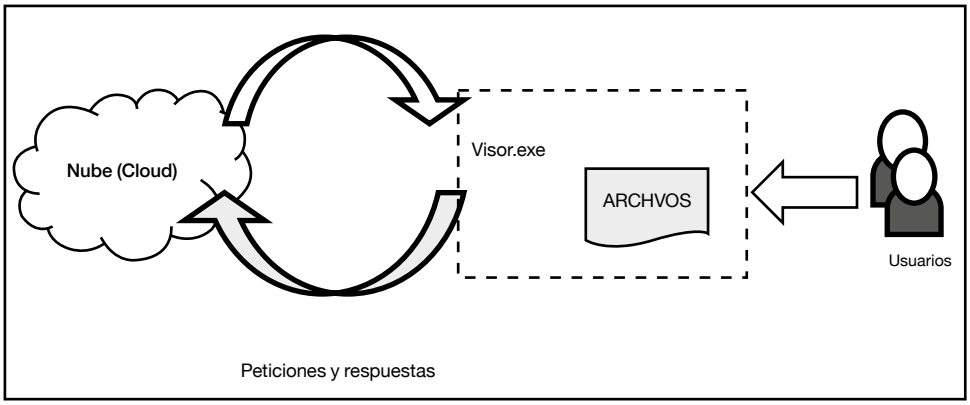

Fig 4. Esquema de un seguidor de datos en CC.

V. FUTURAS INVESTIGACIONES

Dentro del ámbito de la seguridad y protección de la privacidad en CC, se pueden analizar trabajos de confiabilidad en los datos, lo que se conoce como Trusted Computing, trabajos como los de Erickson, (2003) y LaMacchia, (2002), estudian procedimientos para asegurar un seguimiento confiable de los datos hasta un servidor remoto. Trusted Computing podría proporcionar una solución alternativa que garantice que el seguidor de datos no está en peligro; y, en combinación con el trabajo realizado en Ko et al., (2011); Ko, Jagadpramana, & Bu-Sung Lee, (2011); Zhang, Kirchberg, Ko, & Bu Sung Lee, (2011), se muestra cómo mediante el uso de herramientas de monitoreo, diferentes violaciones en las políticas o regulaciones pueden ser notadas y marcadas.

CONCLUSIONES

En este trabajo se analizó diferentes técnicas sobre seguridad de los datos y la privacidad, con la finalidad de conocer los avances actuales y las posibles mejoras para los usuarios de las TIC's.

A pesar de que CC tiene muchas ventajas, todavía existen muchos problemas reales que necesitan ser resueltos. De acuerdo con una encuesta (Deyan Chen & Hong Zhao, 2012) sobre los ingresos de CC, el tamaño del mercado ascenderá a 149 mil millones de dólares para el año 2014, con una tasa de crecimiento anual del 20%. La estimación de ingresos implica que CC es una industria rentable. Pero desde otra perspectiva, las vulnerabilidades existentes en CC son una tentación para las amenazas de los hackers.

Los obstáculos hacia el rápido crecimiento de CC son los problemas de seguridad de datos y privacidad. La reducción de espacio de almacenamiento de datos y el costo de procesamiento de esta información son parámetros

que cualquier organización debe tomar en cuenta, mientras que el análisis de la información es siempre de la tarea más importantes para la toma de decisiones. Un número de técnicas han sido propuestas por los investigadores para la protección de datos y para alcanzar un nivel más alto de seguridad en CC. Sin embargo, todavía hay muchas tareas por hacer para convertir esta tecnología en eficaz y confiable. Son necesarias mayores investigaciones en este campo para garantizar a los usuarios de CC que sus datos estarán seguros.

LITERATURA CITADA

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. Ieee Transactions on Dependable and Secure Computing, 1(1), 11-33.

Bouayad, A., Blilat, A., El Houda Mejhed, N., & El Ghazi, M. (2012). Cloud computing: Security challenges. Information Science and Technology (CIST), 2012 Colloquium In, pp. 26-31.

Deyan Chen, & Hong Zhao. (2012). Data security and privacy protection issues in cloud computing. Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference On, , 1. pp. 647-651.

Erickson, J. S. (2003). Fair use, DRM, and trusted computing. Communications of the ACM, 46(4), 34-39.

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with care an information accountability perspective. IEEE Internet Computing, 15(4), 31-38.

Hurst, D. (2011). Cloud security knowledge 101 [cloud computing security]. Security, 48(3), 94, 96-94, 96.

IBM seguiridad. (2010). Retrieved 11/25/2014, 2014, from http://tupiensas.com/ibm-desarrolla-un-sistema-criptografico-revolucionario/

Karat, J., Karat, C., Brodie, C., & Feng, J. (2005). Privacy in information technology: Designing to enable privacy policy management in organizations. International Journal of Human-Computer Studies, 63(1-2), 153-174.

Kirkham, T., Djemame, K., Kiran, M., Ming Jiang, Armstrong, D., Corrales, M., et al. (2012). Assuring data privacy in cloud transformations. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and

Communications (TrustCom), , 1063-9.

Ko, R. K. L., Jagadpramana, P., & Bu-Sung Lee. (2011). Flogger: A file-centric logger for monitoring file access and transfers within cloud computing environments. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference On, pp. 765-771.

Ko, R. K. L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Qianhui Liang, et al. (2011). TrustCloud: A framework for accountability and trust in cloud computing. Proceedings of the 2011 IEEE World Congress on Services (SERVICES 2011), , 584-8.

LaMacchia, B. A. (2002). Key challenges in DRM: An industry perspective. Digital Rights Management, 2696, 51-60.

Leavitt, N. (2009). Is cloud computing really ready for prime time? Computer, 42(1), 15-20.

Mell, P., & Grance, T. (2010). The NIST definition of cloud computing. Communications of the ACM, 53(6), 50-50.

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. Proceedings of the 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom 2010), , 693; 693-702; 702.

Shacham, H., & Waters, B. (2013). Compact proofs of retrievability. Journal of Cryptology, 26(3), 442-483.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22(5), 847-859.

Yu Shyang Tan, Ko, R. K. L., Jagadpramana, P., Chun Hui Suen, Kirchberg, M., Teck Hooi Lim, et al. (2012). Tracking of data leaving the cloud. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference On, pp. 137-144.

Zeng, K. (2008). Publicly verifiable remote data integrity. Information and Communications Security, Proceedings, 5308, 419-434.

Zhang, O. Q., Kirchberg, M., Ko, R. K. L., & Bu Sung Lee. (2011). How to track your data: The case for cloud computing provenance. Proceedings of the 2011 IEEE 3rd International Conference on Cloud Computing Technology and Science (CloudCom 2011), , 446-53.