Explorando Cloud Forensics

Jose David Oviedo Mercado
Josedom0403@gmail.com
Universidad Piloto De Colombia

Resumen—En el presente artículo se busca entender como cloud forensics analiza y enfrenta los incidentes de seguridad que se presentan en las plataformas de cloud computing y asimismo las dificultades que se exhiben en las investigaciones cuando se tratan de aplicar las técnicas necesarias en estos entornos virtualizados, los cuales cada vez como aspectos legales y contornos geográficos se convierten en preocupaciones que los expertos forenses deben enfrentar con el fin de no infringir en el acceso legal a los datos.

Índice de términos—cloud computing, infraestructura, cloud forensics, csp, software, dimensión.

Abstract— In this article seeks to understand how cloud forensics analyzes and faces security incidents that occur in the cloud computing platforms and also the difficulties shown in investigations when they try to apply the necessary techniques in these virtualized environments, which increasingly as legal and geographical boundaries become concerns that forensic experts must face in order not to infringe on the legal access to the data.

Keywords—cloud computing, infrastructure, cloud forensics, csp, software, dimension.

I. INTRODUCCIÓN

Con el pasar de los años la información se ha convertido en el activo más importante dentro y fuera de las organizaciones a nivel mundial, la automatización de los procesos ha traído consigo grandes cantidades de información, en el cual su almacenamiento ha llevado a las organizaciones a incrementar sus costos en las adquisiciones de infraestructura tecnológica.

Cloud computing surge con el fin de ofrecer y garantizar mediante un servicio el almacenamiento, procesamiento y transmisión de la información de una manera rápida y segura en servidores externos a las organizaciones, reduciendo de manera considerable los costos de la infraestructura tecnológica. Con el auge de esta tecnología los problemas a escalas de análisis forense se han agravado, ya que estos sistemas no son ajenos a intrusiones de red, lo cual puede ocasionar a las organizaciones exponer información confidencial en manos inadecuadas, es por esto que se crea una nueva vía para la investigación con diferentes retos.

Los expertos forenses deben luego tratar de adoptar y desarrollar sus competencias forenses en entornos de computación en la nube, es por eso que el objetivo de este documento es poder explorar las características más significativas, los diferentes usos, las leyes y reglamentos, adicionalmente los grandes desafíos que enfrentan los expertos para tratar que las distintas amenazas que día a día crecen de manera considerable en los diferentes entornos de la nube.

II. DEFINICIÓN

El término de cloud forensics se puede considerar como la disciplina que identifica, analiza y aplica las técnicas forenses en los ecosistemas de cloud computing.

La nist define el término de cloud forensics como "*La aplicación de la ciencia a la identificación, el examen, la recolección y análisis de datos, mientras que la preservación de la información y el mantenimiento de una estricta cadena de custodia de los datos*."[1]

Figura 1. Cloud forensics
http://conexioninversa.blogspot.com/2012/10/cloud-forensics-la-nube-amazon-y-el.html

Esta también es considerada como el subconjunto de la rama forense en la red, en la cual se siguen los principios más importantes de actividades forenses en la red y emplearlos en los ambientes cloud.

III. DIMENSIONES

Cloud forensics posee tres características importantes denominadas dimensiones, en cada una de estas se detallan los procedimientos necesarios para la recolección de evidencias forenses y así poder ser utilizadas en las labores investigativas.

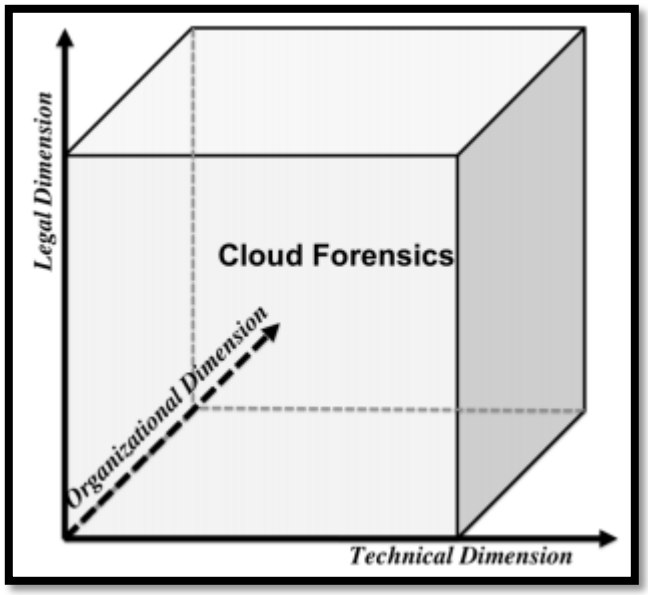

Figura 2. Las 3 dimensiones
http://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000.pdf

Dimensión técnica: Consiste en un conjunto de herramientas y procedimientos necesarios para llevar a cabo el proceso forense en entornos cloud. Esto incluye la recolección de datos forense, la segregación de las pruebas, investigaciones en entornos virtualizados y preparaciones proactivas. [2]

Esta dimensión además exhibe algunos aspectos representativos, los cuales se detallan a continuación:

A. Recopilación de datos forenses: En este proceso se deben identificar, marcar y registrar todos los datos forenses, los cuales serán rotulados para su respectiva investigación.

B. Elastic, static and live forensics: La recolección de los datos volátiles se realizan por medio de herramientas forenses, estas actividades de recaudación son bastantes complejas por la falta de sincronización de las marcas de tiempo.

C. Segregación de la evidencia**:** para los proveedores de la nube y los organismos encargados, deben hacer cumplir la ley cuando se realicen investigaciones, ya que no se debe violentar la confidencialidad de los residentes, teniendo en cuenta que comparten la misma infraestructura.

Dimensión organizacional: En esta dimensión las investigaciones forenses en entornos de computación en la nube siempre implican, al menos, dos partes: el csp, y los clientes de servicios en la nube. [3].

Cada organización debe contar con una estructura organizativa interna, ya que esta garantizara el control de las actividades forenses que se realicen dentro de cada una de las partes, dado el caso de presentarse acontecimientos como accesos no autorizados, perdida de información o denegación de servicio, contar con personal capacitado para el cumplimiento de las siguientes funciones:

A. Investigadores: Son los encargados de las investigaciones y también debe poseer las capacidades para la realización de actividades forenses para poder interactuar con las demás partes.

B. Profesionales: Se encargan de facilitar al investigador el acceso a cada escena que se presente por incidentes de seguridad, lo cual además pueden recolectar evidencias para los investigadores.

C. Grupo de incidentes**:** Estas personas son las encargadas de tratar los incidentes que se presenten en las plataformas de cloud computing, además estos sucesos son manejados de acuerdo a su nivel de criticidad.

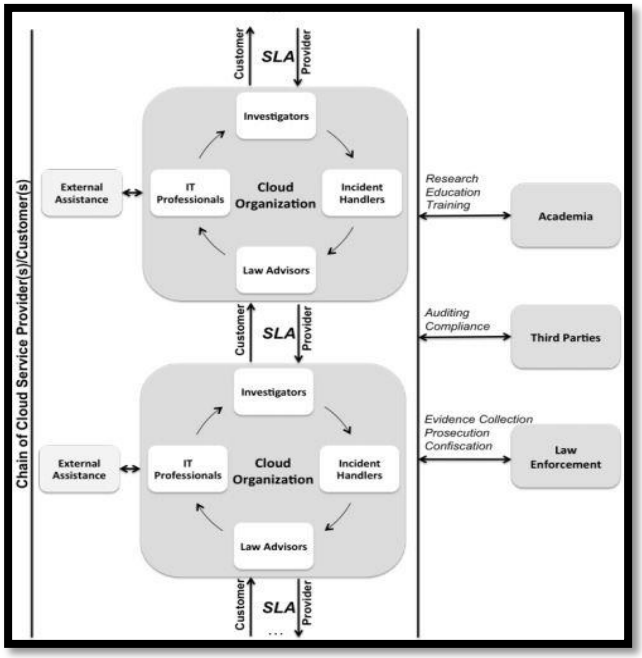

Figura 3.Estructura organizacional cloud forensics

http://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000.pdf

D. Asesores legales: Son los individuos que deben estar encargados de todo el tema multi-jurisdiccionales para que al realizar procedimientos forenses no violen las regulaciones establecidas.

E. Asistencia externa: las organizaciones en la nube deben contar con personal externo para que en conjunto con la estructura organizativa interna permita de manera eficiente los procedimientos forenses.

Cadena de dependencias: Los csp muy a menudo presentan dependencias con otros csp, lo que conlleva a depender de otras investigaciones, es por eso que se debe tener una buena comunicación para así poder colaborarse y facilitar las actividades que se lleven a cabo.

A. Cumplimiento de la ley**:** La falta de comunicación entre las partes llevan a involucrarse en problemas por la recopilación del material probatorio, es por eso que se necesita trabajar estrechamente con las autoridades para poder mejorar las relaciones entre si y además poder confiscar los recursos.

B. Terceros: Todas las organizaciones deben y tienen que trabajar de la mano con terceros para mantener así buenas relaciones, esto ayudará los temas de auditoria y adicionalmente cumplir con las actividades forenses en los entornos cloud computing.

C. Academia: Las organizaciones deben trabajar muy de la mano con la academia, los cuales ayudaran a contribuir con el conocimiento y la capacitación del personal de la estructura interna organizacional.

Dimensión legal: Las investigaciones que se requieran llevar a cabo mediante cloud forensics, lo primero que se debe garantizar es que estas no violaran ninguna ley o reglamento en el área donde se almacena físicamente la información. [4]

Asimismo, se debe tener en cuenta que pueden

existir varias jurisdicciones donde se deben contemplar aspectos legales con otros países, lo cual dificulta la fijación de la cadena de custodia, siendo estas una de las principales preocupaciones para los expertos forenses, ya que, al no disponer del control total de los datos por la poca cooperación de los proveedores de servicios (csp) entorpece la recolección de evidencias, lo que conlleva a la obstaculización completa de la investigación.

Para esta dimensión también se debe tener en cuenta lo siguiente:

A. Multi-jurisdicción y multi-tenencia: Se debe asegurar que las actividades forenses que se realicen, no quebranten las leyes o reglamentos, además se debe cerciorar la confidencialidad de los demás residentes en la infraestructura.

B. Sla: Se deben definir las condiciones del servicio entre el csp y cliente, asimismo, deben quedar establecido en los acuerdos las investigaciones.

IV. APLICACIONES

Esta disciplina nos presenta los diferentes usos y estrategias, las cuales son de gran ayuda para la realización de actividades forenses en la actualidad.

A. Investigación: Aquí se realizan todas las actividades de reconstrucción de eventos al detectarse operaciones sospechosas en los entornos de cloud computing, adicionalmente en adquirir y suministrar las pruebas necesarias antes los tribunales.

B. Solución de problemas: Los expertos que resuelven las dificultades funcionales y operacionales deben desarrollar nuevas estrategias para prevenir que se presenten hechos similares más adelantes.

C. Log: Es la recolección y análisis de todos los registros que se ejecuten a los múltiples servicios alojados en la nube.

D. Datos y recuperación del sistema: La recuperación de los sistemas afectados se debe realizar de forma controlada, ya que requiere una evaluación de los daños causados y así determinar si los datos fueron comprometidos para su posterior recuperación.

E. Cumplimiento normativo: Se debe ayudar al buen cumplimiento de todos los requisitos y así lograr que la información confidencial mantenga su integridad.

V. DESAFÍOS

Los expertos forenses se enfrentan a duros desafíos para la búsqueda de evidencias en ecosistemas cloud, pero las herramientas utilizadas para el levantamiento de las pruebas son muy limitadas.

A. Recolección de datos forenses: Uno de los desafíos más importantes para los expertos es la recolección de los datos forenses, ya que el acceso varía de acuerdo al modelo de la nube donde se presente el incidente. La poca colaboración de parte de los csp y las condiciones en los sla para realizar estos procedimientos hace que las investigaciones se tornen lentas.

B. Personal interno: La estructura organizativa forense no cuenta con la experiencia necesaria para realizar pericia forense, lo que ocasiona que las investigaciones se tornen pesadas en comparación con la evolución de la tecnología, lo cual hace necesario explorar, desarrollar y capacitar al personal para hacer frente a las nuevas formas de ataque en estos entornos.

C. Dependencia externa: La correlación de actividades entre los cps se convierte en un gran reto, porque si no existe coordinación entre las

partes involucradas puede ocasionar que la cadena de custodia se contamine lo que conlleva a un problema en la investigación.

D. Elastic, static and live forensics: Las cargas de trabajo cuando se realizan las investigaciones se pueden complicar por el número de dispositivos que se encuentran conectados en la nube, además la sincronización de la fecha y hora son elementos cruciales para ser utilizados como evidencia en estas labores de exploración.

E. Segregación de la evidencia: La debílidad de resgitro de los modelos cloud sirven de ayuda a los criminales ocultar las identidades, lo cual dificulta a los expertos la identificación y rastreo de los sospechosos.

F. Entornos virtualizados: Los csp utilizan los entornos cloud como instancias virtualizadas, estas instancias funcionan como máquinas virtuales las cuales son monitoreadas y aprovisionadas por medio de un monitor de máquinas virtuales llamado hypervisor. Los atacantes siempre centran los ataques al monitor para poder comprometer la seguridad.

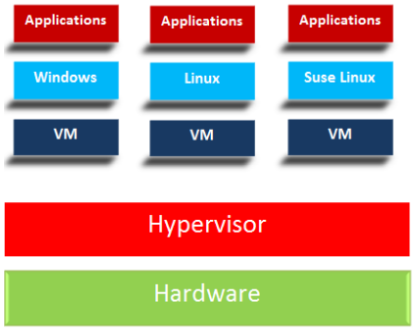

Figura 4. Hypervisor

http://blog.binarymist.net/2012/01/23/bare-metal-hypervisor-setup-evaluation/

G. Sla: Las investigaciones forenses no se incluyen en los sla por la falta de conocimiento del cliente, ya que no tienen la claridad suficiente de los problemas de criminalidad en la nube.

H. Multi-jurisdicción: Las diferencias entre las jurisdicciones afectan las investigaciones que se lleven a cabo, ya que uno de los problemas en el que tipo de datos se puede acceder y adicional es cómo llevar a cabo la recuperación de pruebas sin violar la privacidad o el privilegio de los derechos de los arrendatarios de acuerdo a las políticas de privacidad.

VI. OPORTUNIDADES

A. Costos: Los productos que se prestan para la realización de tareas forenses en los sistemas de cloud computing serán más económicos cuando los servicios se implementen a una escala mayor.

B. Abundancia de datos: Al tener gran cantidad de información ayudara a los expertos forenses a realizar investigaciones en la nube de una manera más eficiente, contando además con altas probabilidades para la recuperación de los datos.

C. Establecimiento de normas: Se debe aprovechar la oportunidad para poder establecer las políticas y estándares que ayuden a tener soluciones más eficientes ya que la nube está aún en sus comienzos.

D. Servicio: Cloud forensics debe ser incluido como un servicio en la nube, para que así pueda facilitar las investigaciones y asegurar en todos los niveles las amenazas informáticas.

E. Escalabilidad y flexibilidad: Las actividades forenses solo se pueden utilizar cuando ocurren incidentes de seguridad en las plataformas cloud, estos sucesos pueden tomar grandes ventajas de la gran medida costo beneficio.

F. Robustez: Algunas tecnologías ayudan a la corpulencia de la ciencia forense, ya que algunos casos como amazon en donde pueden tomar imágenes virtuales en vivo para realizar análisis, reduciendo considerablemente los tiempos de

investigación.

VII. CONCLUSIONES

Cloud forensics en una disciplina que se encuentra en crecimiento, pero los escasos procedimientos y técnicas en las plataformas de cloud computing, hacen ver una disciplina en pañales, la falta de cooperación de las jurisdicciones internacionales y cps dificultan fijar una buena cadena de custodia.

El futuro para esta esta disciplina es muy alentador ya que se tiene mucho para investigar y al igual que otras tecnologías trae oportunidades únicas para establecer políticas y procedimientos, los cuales podrán ser de gran ayuda para los expertos a la hora de la reconstrucción de los hechos.

VIII. REFERENCIAS

[1] Xath Cruz, "Definitions of cloud forensics" http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/. Nov 5 2012

[2] Xath Cruz," The technical dimension" http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/. Nov 5 2012

[3] Keyun Ruan, Prof. Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie, "The organizational dimension" http://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000.pdf

[4] Xath Cruz," The legal dimension http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/. Nov 5 2012

[5] Infosec Institute,"Cloud forensics: an overview" http://resources.infosecinstitute.com/overview-cloud-forensics/

Pedro Sánchez, "Cloud forensics (La nube, amazon y el análisis forense" http://conexioninversa.blogspot.com/2012/10/cloud-forensics-la-nube-amazon-y-el.html

[6] Dominik Birk and Christoph Wegener, "Cloud forensics" http://www.admin-magazine.com/Articles/Cloud-Forensics

[7] NIST "Nist cloud computing forensic science challeng" http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

[8] Kumiko Ogawa "Cloud forensics: an overview" https://www.cs.ucf.edu/~dcm/Teaching/CDA5532-CloudComputing/StudentPresentations/KumikoOgawaP2.pdf

[9] Madan Oberoi, "Cloud forensics" https://prezi.com/zrjdjqbdm7zw/copy-of-cloud-forensics/

Autor
José David Oviedo Mercado
Ing. Sistemas
Est. Especialización En Seguridad Informática
Diplomado Gestión De La Seguridad Y El Riesgo
Universidad Piloto De Colombia
Mayo 2015