Protección del Cloud Computing en seguridad y privacidad

Por el Dr. Javier Areitio

Prof. Dr. Javier Areitio Bertolín – E.Mail: jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE.
Director del Grupo de Investigación Redes y Sistemas.
Universidad de Deusto.

En el presente artículo se aborda una de las áreas tecnológicas de crecimiento e inversión más acusada y con perspectivas de mercado más importantes denominada cloud computing (o simplemente nube). Posibilita el outsourcing de la computación y servicios sin externalizar su control y se basa en utilizar un modelo de pago por uso, con acceso Web a Internet con banda ancha. La industria del cloud computing representa un gran ecosistema con muchos modelos, fabricantes y nichos de mercado. Actualmente se percibe como la necesidad más urgente del paradigma en evolución cloud computing la protección desde sus dos perspectivas de su seguridad y privacidad. Los proveedores de infraestructuras como centros de supercomputación, grandes empresas de telecomunicaciones y empresas de hosting disponen de las tecnologías, herramientas y modelos de gestión para optimizar la asignación de sus recursos ofreciendo nuevas oportunidades de negocio en los mercados emergentes del cloud computing. Ejemplos de proveedores de servicios cloud computing son Google AppsEngine, Amazon Web Services (EC2-Elastic Compute Cloud, S3-Simple Storage Service), GoGrid, FlexiScale, Microsoft Windows-Azure, etc. La protección es el tema capital que exige una solución urgente, evitemos una explosión de incidentes como los de Amazon S3, FlexiScale, gmail, etc.

Cloud computing puede definirse de muy diversas formas:
(a) Describe el empleo de servicios software, almacenamiento o procesamiento que se entregan vía Web desde Centros de Datos masivos. El cloud computing se construye encima de la virtualización.

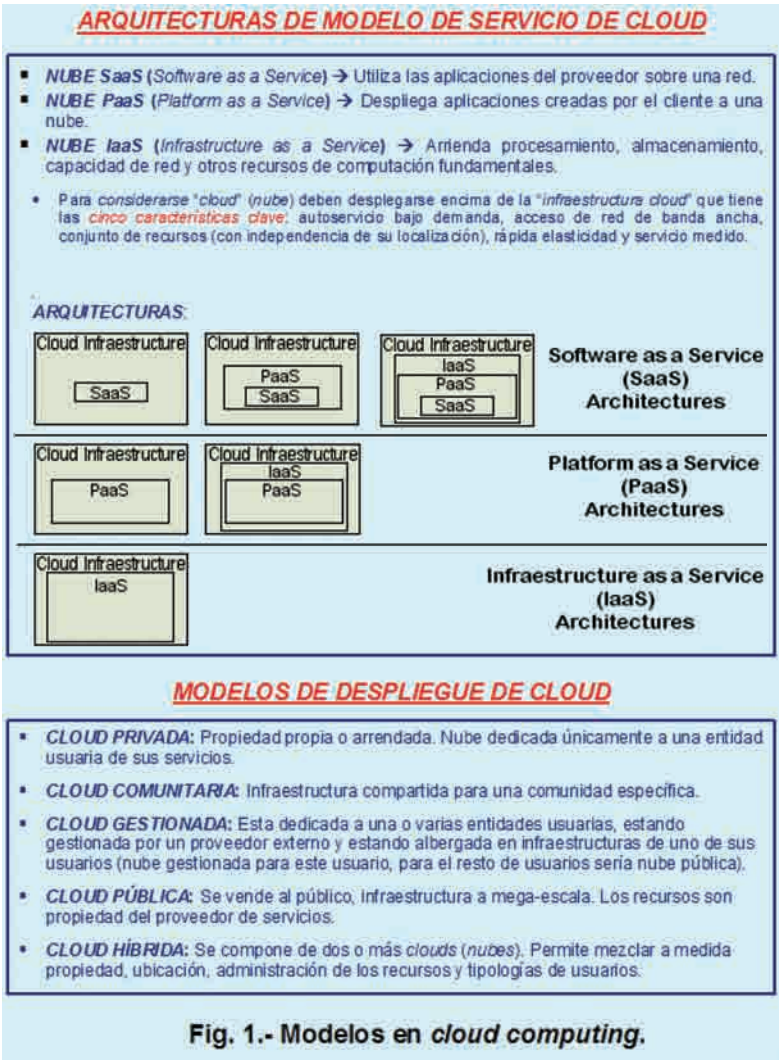

Fig. 1.- Modelos en *cloud computing*.

(b) De un modo más simplificado, consiste en utilizar Internet para todo tipo de necesidades de computación.
(c) Es la realización de Internet basada en el desarrollo y uso de la tecnología de computadores y entregada por un ecosistema de proveedores.
(d) Es la extensión comercial de una utilidad de computación que permite un despliegue elástico de aplicaciones software con alta disponibilidad a la vez que se minimiza el nivel de interacción con la pila tecnológica subyacente.
(e) Un estilo de computación donde las capacidades relacionadas con las TIC (Tecnologías de la Información y las Comunicaciones) se proporcionan de forma masivamente escalable que se facilita como un servicio utilizando las tecnologías de Internet dando soporte a múltiples clientes externos.
(f) Un modelo para permitir un acceso a red conveniente y bajo demanda a un conjunto compartido de recursos de computación configurables (redes, servidores, almacenamientos, aplicaciones y servicios) que pueden proporcionarse rápidamente con un mínimo de esfuerzo de gestión o de interacción del proveedor del servicio (definición del NIST). Este modelo o paradigma de nube promueve la disponibilidad.

Actualmente la catorceava compañía mayor de software por capital de mercado Salesforce.com opera casi enteramente en la nube, las cinco principales compañías de software por

ingresos de ventas tienen ofertas de cloud computing y las previsiones del mercado en su conjunto se espera que crecerán a 160 billones de dólares para el 2011 (fuente Merrill Lynch). Según IDC Enterprise Panel la seguridad es la principal preocupación en torno a este nuevo paradigma. Recientemente IBM ha resultado seleccionado por las Fuerzas Aéreas de Estados Unidos para diseñar y desplegar una infraestructura segura de cloud computing capaz de dar soporte a las redes de inteligencia y defensa. Uno de los proyectos españoles sobre cloud computing es NUBA (Normalized Usage of Business-oriented Architectures) cuyo coordinador es TID (Telefónica I+D), cuenta entre otros con socios como Atos Origin, Centros de supercomputación de Barcelona y Galicia, la UCM, etc. En el OpenCloud Manifesto de 2009 algunos de los principales proveedores de cloud computing indican que debería existir cooperación entre proveedores, libertad de elección para los clientes, flexibilidad en su uso, utilización de estándares necesarios, rapidez y agilidad con posibilidad de introducir mejoras que los clientes precisen y coordinación de esfuerzos entre proveedores.

Modelos en Cloud Computing. Beneficios e inconvenientes.

Cloud computing es una nueva tendencia en TIC que evoluciona muy rápidamente y que se esta haciendo cada vez más popular, representa un cambio importante en la forma en la que se almacenan y ejecutan aplicaciones (aplicaciones de escritorio, aplicaciones y servicios Web) posibilita un autoservicio bajo demanda. Permite mover la computación a la nube. Aunque el concepto no es muy nuevo el término cloud computing aparece como tal en el 2007, sin embargo ya desde hace tiempo utilizamos ciertas formas de cloud computing como por ejemplo las Redes Sociales como Facebook/MySpace y cuentas de correo electrónico basadas en Web como gmail. El cloud computing proporciona una infraestructura eventualmente ilimitada para almacenar y ejecutar datos y programas de clientes. Los clientes no necesitan tener su propia infraestructura, sólo acceso vía Web.

Los principales modelos de despliegue son:

(1) Nube privada. La infraestructura de cloud sólo opera para una organización. Puede gestionarla la propia organización o una tercera parte y puede existir en el local o fuera.

(2) Nube comunitaria. La infraestructura de nube se comparte por parte de varias organizaciones y soporta una comunidad específica que tiene intereses compartidos (por ejemplo misión, requisitos de seguridad, política y consideraciones de cumplimiento). La pueden gestionar las organizaciones o una tercera parte y puede existir en el local o fuera.

(3) Nube pública. La infraestructura de nube se hace disponible al público en general o a un gran grupo industrial y es propiedad de una organización que vende los servicios de cloud computing.

(4) Nube híbrida. La infraestructura de nube es una composición de dos o más nubes (privada, comunitaria o pública) única para las entidades pero se limitan juntas por medio de tecnología propietaria o estandarizada que permite la portabilidad de datos y aplicaciones.

Los principales modelos de servicio son:

(1) Nube SaaS (Software as a Service). La capacidad proporcionada al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en la infraestructura de nube y son accesibles desde diversos dispositivos cliente (PCs-notebooks, teléfonos móviles, iPhones, etc.) utilizando una interfaz cliente ligero como un navegador Web (por ejemplo correo electrónico basado Web o webmail). El consumidor no gestiona, ni controla la infraestructura de nube subyacente, red, servidores, sistemas operativos, almacenamiento, capacidades de cada aplicación individual

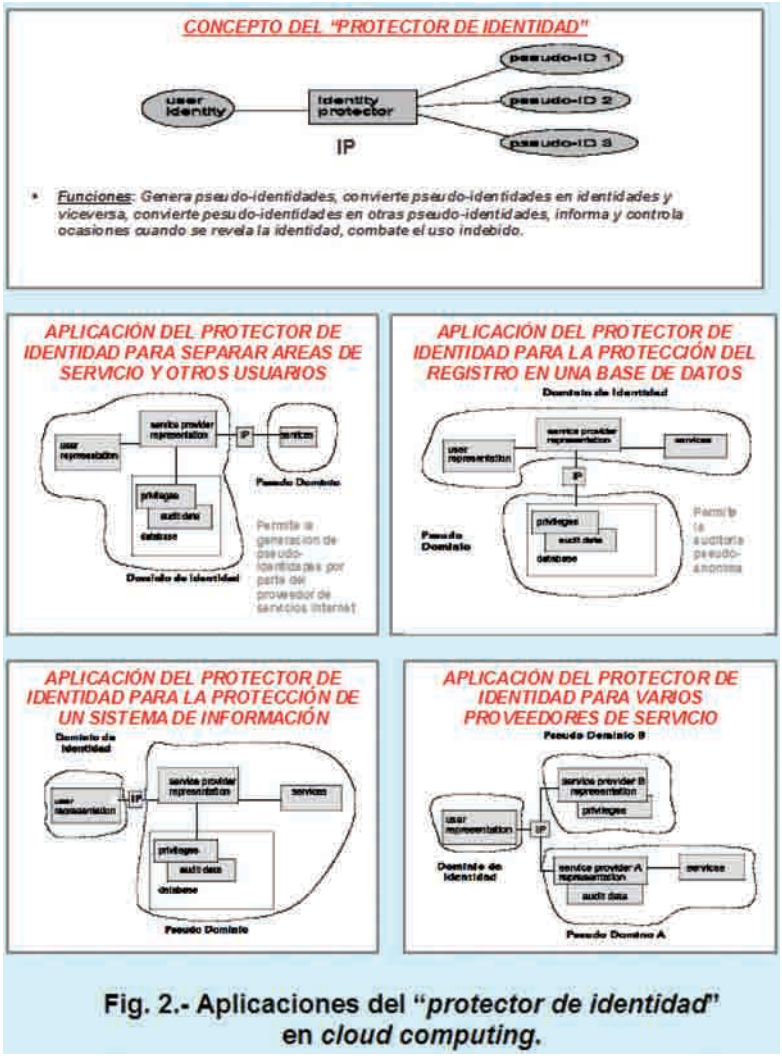

Fig. 2.- Aplicaciones del "*protector de identidad*" en *cloud computing*.

con la posible excepción de establecer de forma limitada la configuración de la aplicación específica del usuario.
(2) Nube PaaS (Platform as a Service). La capacidad proporcionada al consumidor se despliega en las aplicaciones creadas por el consumidor de la infraestructura de nube utilizando lenguajes de programación y herramientas soportadas por el proveedor (como Java, Python, .Net). El cliente no gestiona, ni controla la infraestructura de nube subyacente, red, servidores, sistemas operativos o almacenamiento pero el consumidor tiene control sobre las aplicaciones desplegadas y posiblemente las configuraciones del entorno de hospedaje de la aplicación.
(3) Nube IaaS (Infrastructure as a Service). La capacidad proporcionada al consumidor es la provisión de procesamiento, almacenamiento, redes y otros recursos de computación fundamentales donde el consumidor puede desplegar y ejecutar software arbitrario que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona, ni controla la infraestructura de nube subyacente, pero tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas y posiblemente

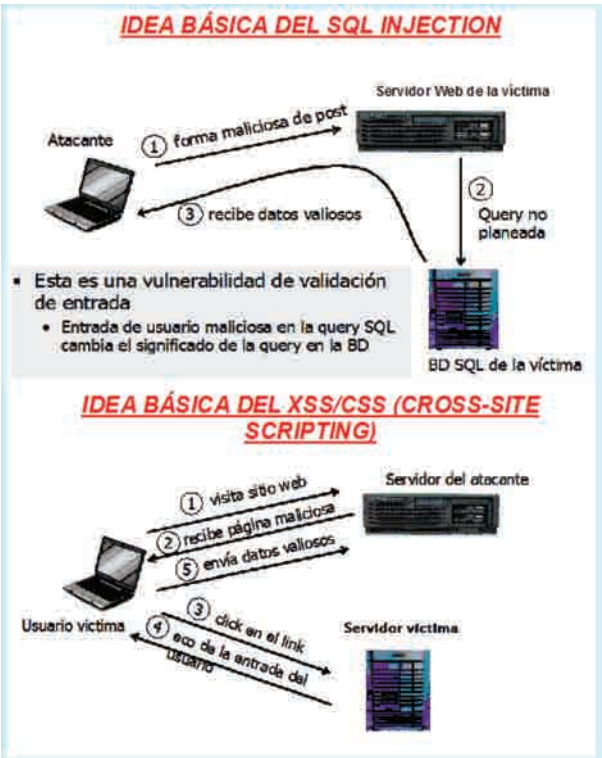

Fig. 3.- Algunos ataques en *cloud computing*.

PRIVACIDAD / PET (PRIVACY ENHANCING TECHNOLOGIES) EN CLOUD COMPUTING

- *INFORMACIÓN RELEVANTE A LA PRIVACIDAD*: Cualquier información relativa a una persona natural identificada o identificable. Una persona identificable es aquella que puede ser identificada directa o indirectamente, en particular por referencia a un número de identificación o a uno o más factores específicos a su identidad física, psicológica, mental, económica, cultural o social (*Directiva UE 95/46/EC-Art. 2*).
- *ALGUNOS ENFOQUES PET*: Anonimato o pseudo-anonimato, desconexión del *PII* (*Personal Identificable Information*). No correlación para dificultar la posible conexión con la *PII*. Evitar la re-identificación (sujetos o sus dispositivos que no puedan ser re-identificados con la ayuda de otros conjuntos de datos. Soportar la confidencialidad basada en criptografía y *esteganografía*. Implantar políticas de notificación fehacientes y de elección por parte del usuario (políticas de privacidad estrictas).
- *ASPECTOS PET*: (A) *Protección de las identidades de usuario en el nivel de comunicaciones*. Implantando: (1) Anonimato/pseudo anonimato del emisor utilizando tráfico de mosqueo, *DC-Nets*, *Crowds*, etc. (2) No correlación entre emisor y receptor en base al uso de *Mix-Nets*. Empleo de no observabilidad del usuario con esteganografía. (3) Anonimato/pseudoanonimato del receptor utilizando difusión de mensajes y direcciones implícitas. Una dirección explícita es la que se coloca en la red como *IP/L3* (*194.56.76.12*) o *MAC/L2* (*FA4BC891D453*) o *URL/L5* (*http://www.anonymizer.com proxy Web* que filtra la dirección IP origen del navegador, nombre usuario, filtra *Applets Java*, *JavaScripts*, *cookies*, etc.). Una *dirección implícita* es un atributo que puede ser reconocido por la entidad direccionada. Una *dirección implícita invisible* sólo es visible a su entidad direccionada (se puede realizar utilizando cifrado de *clave pública/asimétrico* o de tipo *simétrico*). Una dirección implícita visible es visible para todos los usuarios (se realiza por medio de pseudónimos auto-escogidos como prefijos del mensaje. Dirección pública es aquella conocida por todos los usuarios. Dirección privada es aquella que el emisor la recibió secretamente de la entidad direccionada. Un *identificador pseudónimo* puede ser una dirección IP dinámica generada por un *servidor DHCP*. (B) Protección de las identidades de los que utilizan datos privados, en base al anonimato/pseudo-anonimato de los sujetos que utilizan los datos. (C) Protección de la confidencialidad e integridad de los datos personales, en base al cifrado, *esteganografía*, *firmas digitales*, funciones *hash*, etc.

RIESGO DE LA RE-IDENTIFICACIÓN. Los registros de datos recogidos para propósitos estadísticos contienen *datos de identidad* (nombre, direcciones, DNI), *datos demográficos* (sexo, *edad*, *raza*, *nacionalidad*), *datos de análisis* (hábitos, enfermedades). El grado de anonimato de los datos estadísticos depende del tamaño de la BD, la entropía de los atributos de datos demográficos que pueden servir como conocimiento suplementario de un atacante. La entropía de los atributos de los datos demográficos depende del número de atributos, del número de valores posibles de cada atributo, de la distribución de frecuencia de los valores y de las dependencias entre atributos. Dado el *atributo nacionalidad* con dos posibles valores: Española (E) y Francesa (F), con probabilidades p(E) = 0,9, p(F) = 0,1 → *Entropía del atributo nacionalidad* = *H(nacionalidad)* = $p(E).\log_2(1/p(E)) + p(F).\log_2(1/p(F)) = 0,465$. El *ANVC* (*Average Number of Value Combinations*) mide el número medio de combinaciones de valores para un conjunto de atributos que pueden utilizarse para la re-identificación: Dados H(raza) = 0,997 y H(sexo) = 0,465 → $ANVC(raza) = 2^{0,997} = 1,996$; $ANVC(sexo) = 2^{0,465} = 1,38$. Si no existen dependencias entre atributos: $ANVC(raza, sexo) = 2^{0,997} \cdot 2^{0,465} = 2,74$. Para *estimar el riesgo medio de re-identificación se usa RR* = (*ANVC* / N). Dada una BD de N = 100 registros para N individuos diferentes si *H(sexo, estado civil)* = 2,61 → $ANVC(sexo, estado\ civil) = 2^{2,61} = 6,105$ → *RR* = 6,105 / 100 = *0,0615* → Estimación del porcentaje de individuos re-identificables = 0,0615 . 100% = 6,15%. Donde $\log_2 x = (\log_{10} x / \log_{10} 2)$.

Fig. 4.- Proteger la privacidad en *cloud computing*.

sobre componentes de red seleccionados (como firewalls, balanceadores de carga, etc.).

Los principales beneficios que puede aportar el cloud computing son:
(a) Minimiza el gasto de capital. Reduce el costo de propiedad (infraestructura como hardware y software) y mantenimiento.
(b) Independencia de localización y dispositivo.
(c) Mejora de utilización y eficiencia.
(d) Escalabilidad y elasticidad muy alta.
(e) Potencia de computación elevada.
(f) Nuevas formas de colaboración de grupo.
(g) No necesita espacio físico para almacenar servidores y bases de datos ya que están en la nube.
(h) Independencia de sistemas operativos y virtualmente capacidad de almacenamiento ilimitada.

Los principales inconvenientes que pueden identificarse en el cloud computing son:
(a) El primero y más urgente es la protección de la seguridad y privacidad de datos y programas.
(b) Carencia de control.
(c) Fiabilidad cuestionada.
(d) Única limitación el acceso a Internet que se quede sin conexión o que las conexiones se hagan de baja velocidad.
(g) La no portabilidad de una aplicación construida para un servido de nube a otro proveedor de servicios de cloud computing.

Problemas de seguridad y privacidad en cloud computing

El cloud computing presenta los mismos problemas de los sistemas convencionales más otros muchos nuevos específicos.

- **EXISTENCIA DE DIFERENTES NIVELES DE SEGURIDAD**: Seguridad de acceso al servidor, seguridad de acceso a Internet, seguridad de acceso a bases de datos, privacidad de datos, seguridad de acceso a los programas. Se debe poder establecer niveles de seguridad tanto a los datos como al código. Se debe poder almacenar los datos de forma redundante en múltiples localizaciones físicas y se debe poder elegir si la localización física debería distribuirse a lo largo de distintos países o dentro de un único país.
- **EN REFERENCIA AL CENTRO DE DATOS DEL PROVEEDOR DE CLOUD COMPUTING**. Se debe considerar que el personal profesional de seguridad utilice video-vigilancia, sistemas IDS/IPS y otros medios electrónicos de monitorización. Cuando un empleado deje un *Centro de Datos* sus privilegios de acceso deberían ser inmediatamente revocados. Todos los accesos físicos y electrónicos de los empleados a los *Centros de Datos* deberían registrarse (*logging*) y auditarse rutinariamente. Deben existir herramientas de auditoría disponibles para que los usuarios puedan fácilmente determinar de que forma sus datos se almacenan, protegen, utilizan y verifican la aplicación de la política establecida.
- **EN RELACIÓN A LA LOCALIZACIÓN DE LOS DATOS**. Cuando un usuario utiliza la nube, el usuario probablemente no sepa exactamente donde se hospedan sus datos y en que país serán almacenados. Los datos deberían almacenarse y procesarse sólo en jurisdicciones específicas definidas por el usuario. El proveedor también debería tener un compromiso contractual para obedecer requisitos de privacidad local en nombre de sus clientes. Deben existir *políticas centradas en los datos* que se generan cuando un usuario proporciona información personal o sensible que viaja a lo largo de todo su tiempo de vida para asegurar que la información sólo se utilice de acuerdo con la política establecida. La *independencia de datos* en *cloud computing* permite añadir al *contenido* de los datos *contexto* que son *atributos* (estructura de significado, información de seguridad/acceso embebida y entendimiento semántico común) de modo que el navegador sabe cuando preguntar por información adicional antes de mostrar más al usuario (esto ocurre con ficheros de música e imágenes protegidas).
- **BACKUPS DE DATOS**. Los datos almacenados en BD del proveedor deberían ser almacenados de forma redundante en muchas localizaciones físicas. Los datos que se generan durante la ejecución de un programa en instancias son datos del cliente y por tanto el proveedor no debería realizar backups (copias de seguridad). Debe existir un control del administrador en las BD.
- **SANEADO DE DATOS**. Es el proceso de eliminar información sensible de un dispositivo de almacenamiento. Las cuestiones que se plantean son: (i) Qué *sucede a los datos almacenados* en un entorno *cloud computing* una vez que haya pasado su "tiempo de uso" por parte del usuario. (ii) Qué *prácticas de saneado* de datos realizará el proveedor de la nube para retirar los datos primarios y redundantes de los dispositivos de almacenamiento y cuando dichos dispositivos se retiran o se sacan de servicio.
- **CUESTIONES DE SEGURIDAD**. El computador que ejecuta el trabajo, el trabajo puede ser un virus o gusano que puede destruir el sistema. Como solución se define un conjunto confiable de usuarios utilizando la distribución de certificados digitales, contraseñas, claves, etc. y luego se definen políticas de control de acceso para permitir que los usuarios confiables accedan a los recursos de los computadores. Algunos virus y gusanos crean inanición de trabajos (donde un trabajo toma una cantidad enorme de recursos lo que resulta en una inanición de recursos para otros trabajos); como soluciones la reserva de recursos y la reducción de prioridad. La seguridad relacionada con la información intercambiada entre diferentes máquinas o entre maquinas y usuarios. Esta cuestión pertenece a la comunicación segura, autenticación y otros aspectos como SSO y delegación. La comunicación segura incluye los aspectos de protección de la comunicación entre dos entidades. La confidencialidad indica que todos los datos enviados por usuarios deberían ser accesibles sólo a receptores autorizados y la integridad indica que todos los datos recibidos sólo deberían ser enviados/modificados por emisores legítimos. Como soluciones el cifrado asimétrico, los certificados X.509v3, SSL/TLS permite autenticación segura y comunicaciones protegidas en redes. En el ataque DoS los servidores y redes se saturan por una gran cantidad de tráfico con lo que a los usuarios se les deniega el acceso a ciertos servicios Internet. La violación QoS esta relacionada con la congestión, retardo o desecho de paquetes o hacking de recursos. El ataque MITM puede neutralizarse con SSL/TLS. El IP spoofing es la creación de paquetes IP utilizando direcciones IP de otras entidades, como solución la infraestructura no debe permitir que una instancia envíe tráfico con una dirección IP o MAC que no son la propia. Un cliente es vulnerable al port scanning cuando configura el grupo de seguridad para permitir tráfico de cualquier origen a un puerto específico, cuando se detecta debería detenerse y bloquearse. En el ataque a la caché ARP, un adversario colocado en la misma red Ethernet puede capturar con un sniffer trafico de red de una víctima en su red y enviar mensajes ARP falsificados a la víctima. El protocolo ARP permite encontrar la dirección MAC asociada a una dirección IP concreta, un computador consulta a la caché o bien si ha expirado el tiempo envía por difusión una petición ARP.

Fig. 5.- Seguridad-privacidad en *cloud computing*.

Entre los más relevantes se pueden identificar:

(1) Vulnerabilidades en el proveedor de cloud computing. Pueden ser a nivel de plataforma como inyección SQL o XSS (Cross-Site Scripting). Se han dado en Salesforce.com, Google Docs. Como posibles contramedidas la herramienta de IBM AppScan que explora vulnerabilidades en servicios Web como un servicio de seguridad de nube.

(2) Ataques a nivel de VM. Un problema potencial en arquitecturas de multi-arrendamiento son las posibles vulnerabilidades en el hipervisor o tecnología VM (Virtual Machine) utilizada por los proveedores de nubes. Han aparecido y seguirán apareciendo vulnerabilidades en VMware, Xen, Virtual PC y Virtual Server de Microsoft. Algunas formas de mitigar estas vulnerabilidades son los parches, la monitorización y los IDS/IPS/firewall.

(3) Phishing/Scams en proveedores de cloud computing. Un ejemplo es el caso del incidente de phishing de Salesforce. Como contramedidas utilizar herramientas anti-fraude/ingeniería social.

(4) Dificultad para realizar análisis forense en la nube. En entornos cloud computing la probabilidad de que los datos sean eliminados, sobrescritos, borrados o destruidos es muy elevada ya que se trata de una infraestructura abierta multi-servidor.

(5) Dificultad para la autenticación y autorización. La autenticación y autorización a nivel de empresa no se extiende a la nube de forma sencilla. Las políticas y métricas propias de una compañía son difíciles y a veces imposibles de integrar con la seguridad de la nube para poder incluir recursos de nube.

(6) Expansión de la superficie de ataque de red. El usuario de una nube debe proteger la infraestructura utilizada para conectarse e interaccionar con la nube, tarea muy complicada ya que la nube esta fuera de los mecanismos de seguridad perimétricos como IDS/IPS/Firewall. Es posible que la nube pueda atacar la máquina que se conecta a ella.

(7) Único punto de fallo. Los servicios de nube se han anunciado bajo el lema que proporcionan más disponibilidad, pero quizás igual estemos equivocados, existen de hecho más puntos únicos de fallo y ataque. Posibles contramedidas redundar equipos, enlaces de comunicaciones y software por si aparecen fallos fortuitos o provocados.

(8) Dificultad para el aseguramiento de la integridad computacional. Puede una empresa asegurarse que un proveedor de nube esta ejecutando de forma defectuosa una aplicación hospedad y dar resultados válidos. Una posible contramedida se propone en el Proyecto Holding@Home de Stanford que da la misma tarea a múltiples clientes para alcanzar un consenso sobre el correcto resultado.

(9) Impacto en el uptime y no poder escalar lo suficiente para poder ejecutar ciertas aplicaciones cuando el colectivo de clientes es muy elevado y continuo con el colapso consiguiente de la nube.

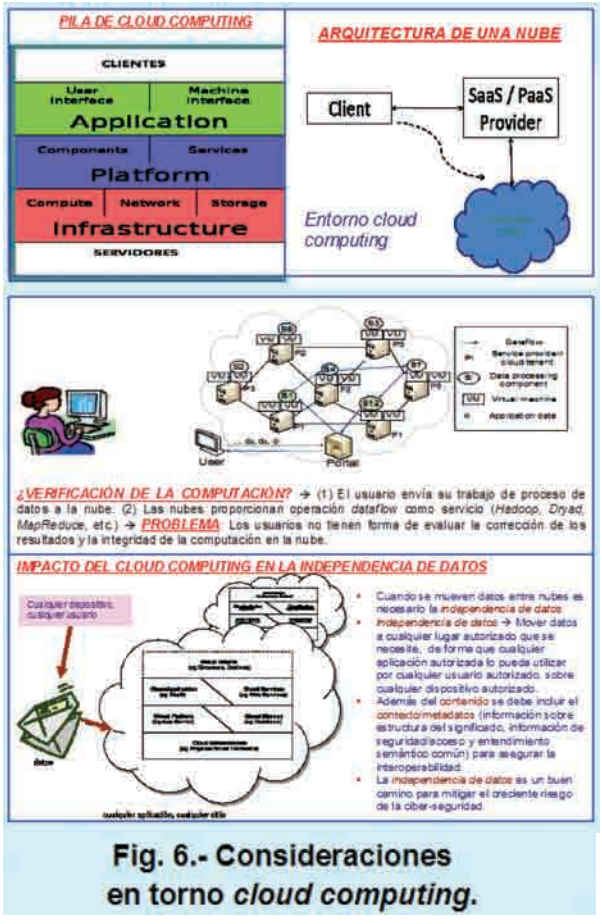

Fig. 6.- Consideraciones en torno *cloud computing*.

(10) Difícil generación de auditorias. Es un efecto colateral de la carencia de control en la nube. No existe suficiente transparencia en las operaciones del proveedor de la nube a nivel de auditoría.
(11) Espionaje en el proveedor de la nube. Y robo de información corporativa. En Facebook los usuarios dejan datos sensibles y convencionales, estos datos los utiliza Facebook para presentarlos a otros usuarios y también los utilizan aplicaciones de terceras partes que se ejecutan en la plataforma. Se podrían crear aplicaciones maliciosas y ejecutarlas en la nube Facebook para robar datos sensibles.
(12) Problemas que plantea la propiedad transitiva. Un proveedor de nube contratado puede realizar subcontratas sobre las que el usuario de la nube tiene menos o ningún control y que pueden no ser de confianza. Caso de los servicios Linkup y Nirvanix.
(13) Demasiados datos para obtener correlaciones. El crecimiento del cloud computing ha creado enormes conjuntos de datos que pueden monitorizarse por aplicaciones como las de las empresas de marketing/anuncios. Por ejemplo Google utiliza su infraestructura de nube para recoger y analizar datos de clientes para su red de anuncios utilizando minería de datos. Si se comparten datos con otras partes es conveniente anonimizarlos.
(14) Nulo control sobre la diligencia de las operaciones de proveedor. Un proveedor de nube no puede garantizar a un usuario que ha borrado datos no deseados o que almacena correctamente los datos del cliente.
(15) No claridad en relación a las obligaciones contractuales. Un proveedor podría violar patentes.
(16) Carencia de interoperabilidad entre nubes. Un usuario de datos que contrata con una nube no puede pasarse a otra nube debido a la existencia de formatos propietarios y vulnerabilidades en APIs.

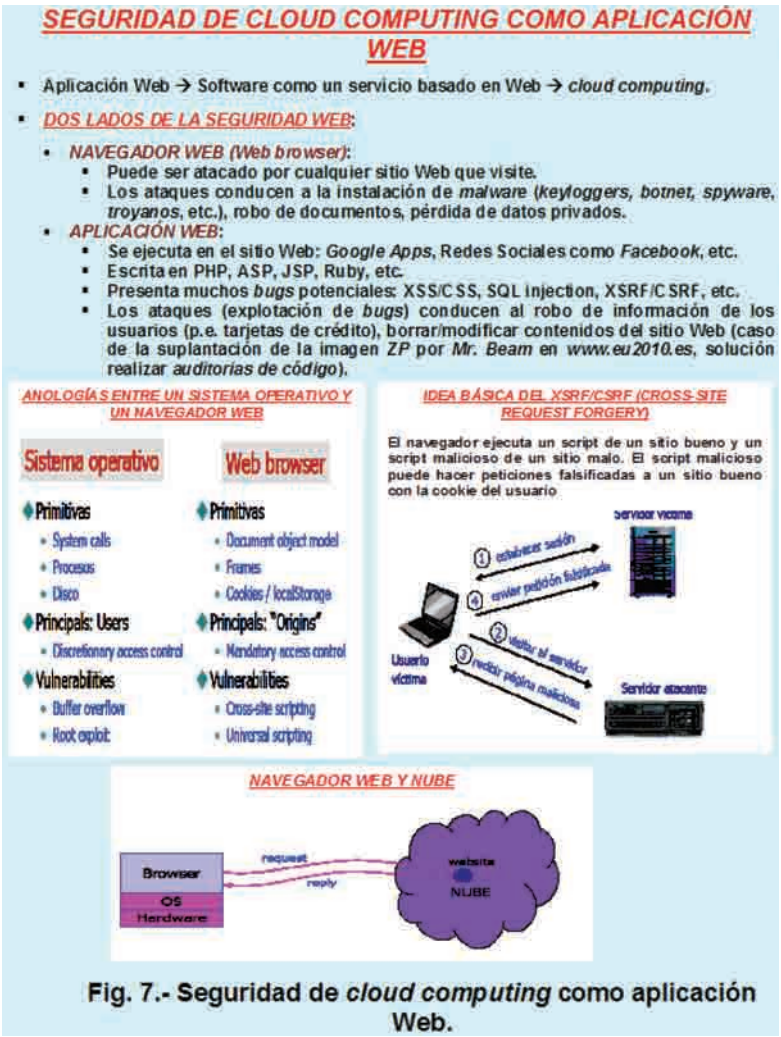

Fig. 7.- Seguridad de *cloud computing* como aplicación Web.

Componentes cloud relevantes a la seguridad.

El cloud computing es actualmente la noción más popular en TIC, sus elementos de elasticidad más relevantes son: el almacenamiento, el procesamiento y las redes virtuales. Como elementos fundamentales del cloud computing se pueden identificar:
(a) Tecnologías primarias: virtualización, tecnología GRID, las arquitecturas orientadas al servicio o SOA, la computación distribuida, las redes de banda ancha, el navegador como plataforma, el software open source y gratuito.
(b) Otras tecnologías: Web 2.0, SLAs (Service Level Agreements), sistemas autonómicos, frameworks de aplicaciones Web, etc. Los SLAs son contratos entre clientes y proveedores de servicio referentes al nivel de servicio que van a proporcionar (ver http://www.sla-zone.co.uk/). Contienen métricas de rendimiento, por ejemplo caudal, tiempo de respuesta, tiempo operativo, uptime. Documenta las capacidades de seguridad-privacidad, detalla la gestión de problemas y contiene penalizaciones por parte del proveedor en caso de no cumplimiento en seguridad, rendimiento, privacidad, etc.

Se pueden identificar como principales componentes cloud desde la perspectiva de la seguridad:

(1) Servicios de aprovisionamiento cloud. Las ventajas principales que puede aportar son la rápida reconstitución de servicios, permite la disponibilidad (provisión en múltiples centros de datos de múltiples instancias) y las capacidades de honey-net avanzadas. Como principales desafíos identificados, el impacto de comprometer el servicio de aprovisionamiento.

(2) Servicios de almacenamiento de datos cloud. Las ventajas principales que puede aportar son la fragmentación y dispersión de datos, la replicación automatizada, la provisión de zonas de datos (por ejemplo por país), el cifrado en reposo y en tránsito y la retención automatizada de datos. Como principales desafíos identificados, la gestión del aislamiento y el multi-arrendamiento de datos, el controlador de almacenamiento (presenta un único punto de fallo en caso de verse comprometido) y la exposición de datos a posibles gobiernos extranjeros.

(3) Infraestructura de procesamiento cloud. Las ventajas principales que puede aportar son la capacidad para proteger masters y sacar imágenes seguras. Como principales desafíos identificados, el multi-arrendamiento de aplicaciones, la dependencia en los hipervisores y el aislamiento de procesos y los mecanismos de sandbox para aplicaciones.
(4) Servicios de soporte cloud. Las ventajas principales que puede aportar son los controles de seguridad bajo demanda, por ejemplo la autenticación, el logging, los firewalls, etc. Como principales desafíos identificados, el riesgo adicional cuando se integra con aplicaciones del cliente, las necesidades de certificación y acreditación como aplicación separada y las actualizaciones de código.
(5) Seguridad perimétrica y de red cloud. Las ventajas principales que puede aportar son la protección contra la denegación de servicios distribuida o DDoS, las capacidades VLAN, la seguridad perimétrica como IAM/IDS/IPS, firewall, autenticación, etc. Como principales desafíos identificados, las zonas virtuales con movilidad de aplicaciones.

Los principales retos en seguridad del cloud computing son:
(a) Necesidad de gestión del aislamiento.
(b) El multi-arrendamiento.
(c) Los retos del registro o logging.
(d) Las cuestiones de propiedad de los datos.
(e) Las garantías de calidad de servicio o QoS.
(f) La dispersión de datos y las leyes de privacidad internacionales como por ejemplo la Directiva Europea de Protección de Datos y el Programa norteamericano Safe Harbor, la exposición de datos a gobiernos extranjeros y las citaciones de datos y las cuestiones de retención de datos.
(g) La dependencia en supervisores seguros.
(h) La atracción de todo tipo de atacantes debido al elevado valor del objetivo que es la "nube".
(i) La seguridad de sistemas operativos virtuales en la nube.
(j) La posibilidad de fallos masivos.
(k) Necesidades de cifrado en cloud computing: cifrado para el acceso a la interfaz de control de recursos de la red, cifrado administrativo de acceso a las instancias de sistemas operativos, cifrado de acceso a las aplicaciones, cifrado de los datos de las aplicaciones en reposo-almacenamiento y tránsito.
(l) Seguridad de la nube pública en contraposición con la seguridad de la nube interna-privada.
(m) Carencia de control de versión SaaS pública.
(n) Problemas con el movimiento de PII (Personal Identificable Information) y datos sensibles a la nube (valoración del impacto de la privacidad).
(o) Utilizar SLAs para obtener seguridad de nube (requisitos sugeridos para SLAs de nube, cuestiones relacionadas con análisis forense en cloud).
(p) Planificación de contingencias y recuperación de desastres para implementaciones de nube.
(q) Gestión de cumplimientos como SOX, PCI-DSS, HIPAA, FISMA, etc.
(r) Auditorias por ejemplo del tipo SAS 70.

Entre las principales cuestiones de privacidad del cloud computing:
(1) Desde la perspectiva de los individuos que se conectan a la nube: maximizar el control de usuario individual, crear servicios anónimos para usuarios individuales, crear mecanismos para el uso de identidades múltiples y limitar la información de identidad y autenticación para transacciones de alto nivel.
(2) Desde la perspectiva de los proveedores de cloud computing: anonimato de la información personal, cifrar datos si contienen información personal, compartimentar-aislar el procesamiento y almacenamiento de datos, controlar los identificadores únicos, gestionar explícitamente los requisitos de seguridad y privacidad entre los proveedores de servicios cloud computing.
(3) Desde una perspectiva global: proporcionar un aviso adecuado so-

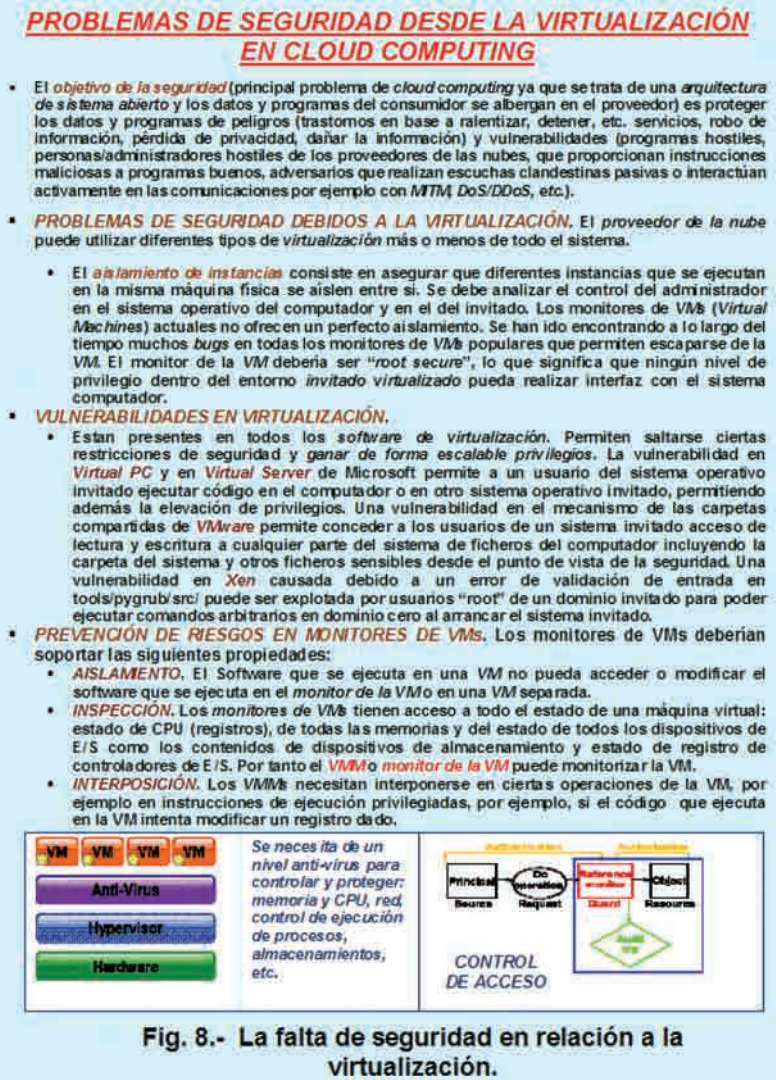

Fig. 8.- La falta de seguridad en relación a la virtualización.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto LEFIS-APTICE (financiado por Socrates. European Commission).

bre la privacidad, soportar el desarrollo de PET (Privacy Enhacing Technologies), utilizar la valoración del impacto de la privacidad y coordinar la aplicación de la privacidad y el cumplimiento a través de diferentes áreas jurisdiccionales (por ejemplo, cuando se pasa de un país europeo a un paraíso fiscal). Si los clientes emprenden procesos del tipo test de penetración no suele ser una buena opción en entornos outsourcing como cloud computing ya que el proveedor de la nube no puede distinguir nuestros test con un ataque real y además nuestros test de penetración pueden potencialmente impactar negativamente en otros usuarios de forma inaceptable.

Consideraciones finales

Nuestro grupo de investigación lleva trabajado casi diez y seis años en el área de la seguridad y privacidad en cloud computing. Del análisis de la seguridad de la nube se han detectado cuestiones clave como confiabilidad, multi-arrendamiento, cifrado no convencional, problemas de cumplimiento, IAM, cuestiones de integridad de datos, códigos y procesamientos.

Bibliografia

- Areitio, J. "Seguridad de la Información: Redes, Informática y SI". Cengage Learning-Paraninfo. 2009.
- Areitio, J. "Análisis en torno a los esquemas de compromiso digital y su aplicación en seguridad de red". REE. Nº 644/645. Julio-Agosto 2008.
- Areitio, J. "Análisis en torno a la auditoria de seguridad en tecnologías de la información y las comunicaciones". REE. Nº 625. Diciembre 2006.
- Areitio, J. "Test de penetración y gestión de vulnerabilidades, estrategias clave para evaluar la seguridad de red". REE. Nº 653. Abril 2009.
- Areitio, J. "Tipificación de amenazas, identificación de contramedidas de seguridad en el ámbito de gestión de redes y sistemas". REE. Nº 613. Dic. 2005.
- Areitio, J. "Identificación de la tecnología firewall para la protección de la seguridad de red". REE. Nº 638. Enero 2008.
- Buffington, J. "Data Protection for Virtual Data Centers". Sybex. 2010.
- Mather, T., Kumaraswamy, S. and Latif, S. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance". O'Reilly Media. 2009.
- Marchini, R. "Cloud Computing: A Practical Introduction to the Legal Issues". BSI Standards. 2010.
- OpenCloud Manifesto: http://www.opencloudmanifesto.org/.
- Reese, G. "Cloud Application Architectures: Building Applications and Infrastructure in the Cloud". O'Reilly Media. 2009.
- Linthicum, D.S. "Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide". Addison-Wesley Professional. 2009.
- Amazon Web Services: http://www.developer.amazonwebservices.com/, http://aws.amazon.com/ec2/.
- Chakrabarti, A. "Grid Computing Security". Springer. 2007.
- Cloud Security Alliance (CSA): http://www.cloudsecurityalliance.org/.
- Hoopes, J. "Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis and Honeypotting". Syngress. 2008.
- Rittinghouse, J. and Ransome, J. "Cloud Computing: Implementation, Management and Security". CRC Press. 2009.
- Krutz, R.L. and Vines, R.D. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing". Wiley. 2010.
- Fingar, P. "Dot Cloud: The 21st Century Business Platform Built on Cloud Computing". Meghan-Kiffer Press. 2009.
- Norman, T.L. "Risk Analysis and Security Countermeasure Selection". CRC Press. 2010.