Cloud Computing y Seguridad

David González
NeoMetrics
Email: david.gonzalez@neo-metrics.com

Julio Rilo
Inixa
Email: julio@inixa.com

***Abstract*—La computación en la nube se presenta como una nueva oportunidad tanto de negocio para las empresas como de investigación en aspectos de seguridad, pero al mismo tiempo plantea un nuevo escenario y nuevos retos. En este artículo, en parte tipo survey y en parte artículo de posición, presentamos algunos de los problemas surgidos y mostramos algunas soluciones que se han desarrollado, haciendo una revisión de algunas nuevas líneas de investigación que han aparecido ligadas a la computación en la nube, y planteamos la necesidad de modificar las soluciones de seguridad anteriores y de conseguir nuevas herramientas especialmente diseñadas para su utilización en el nuevo contexto.**

I. Introducción

La computación en la nube, *Cloud Computing*, ha planteado un escenario nuevo en el campo de las tecnologías de la información, abriendo nuevas líneas de investigación y prometedoras oportunidades, tanto económicas como tecnológicas.

En la actualidad nuestros datos no están protegidos, como venía ocurriendo, dentro de centros de procesos de datos corporativos, aislados de forma física y lógica en espacios y redes de comunicación de ámbito local, gestionados y controlados por personal de nuestra organización y protegidos por cortafuegos, filtros de acceso y medidas de seguridad tradicionales.

Los datos tienden a residir cada vez más en dispositivos móviles y terceros proveedores de la nube. Por una parte, se ha generalizado el uso de todo tipo de dispositivos electrónicos de última generación, con gran capacidad de almacenamiento y proceso (Smartphones, Tablets, Tarjetas SD, etc.), pero que adolecen, en muchas ocasiones, de medidas de seguridad insuficientes para proteger dicha información. Por otra parte, los datos se encuentran en última instancia alojados en espacios y localizaciones que desconocemos y con acceso por parte de personal de terceros que no siguen necesariamente las políticas de seguridad corporativas (procedimentales, legales, etc.).

En este contexto los métodos y técnicas de protección tradicionales no cumplen su función y no previenen de forma adecuada contra fugas de información, accesos no autorizados o ataques del tipo *man in the middle*. Se están abriendo, o en muchos casos reabriendo, nuevas brechas en materia de confidencialidad e integridad de nuestra información. También, aunque pudiera parecer lo contrario por la alta disponibilidad de servicios que vienen ofreciendo los proveedores de Cloud, han surgido problemas de disponibilidad, pudiendo impedirnos el acceso a nuestra información, como han puesto de relieve los recientes casos de cierres de centros de procesos de datos realizados por el FBI.

La nueva situación genera nuevos riesgos y son necesarias, por tanto, nuevas medidas de seguridad en aspectos técnicos, legales y organizativos, ya que el modelo actual de seguridad carece, en la mayoría de las ocasiones, de la eficiencia y efectividad necesarias en este nuevo modelo de computación.

II. Estado del arte

Actualmente se siguen utilizando en la nube técnicas clásicas (es decir, de criptografía actual) de cifrado y protección de datos, pero es cada vez mas claro que la nube plantea nuevos retos que deben ser abordados con nuevas herramientas o bien con adecuadas modificaciones de las herramientas "tradicionales" para adaptarlas a la nueva situación.

De acuerdo con el National Institute of Standards and technology, NIST, la computación en la nube es un modelo que permite disponer de recursos compartidos de computación, a demanda y rápidamente, requiriendo mínimos esfuerzos de administración y mantenimiento y escasa interacción con el proveedor.

La computación en la nube ofrece en la actualidad tres modelos de servicio:

- *Software as a Service* (SaaS), que es el tipo más restrictivo para los usuarios de la nube, pues los proveedores tienen control total sobre los recursos virtuales. El usuario hace uso de un servicio gestionado por el proveedor de la nube, accediendo tras su identificación.
- *Platform as a Service* (PaaS), en el que se ofrece la capacidad de computación en la nube y la posibilidad de usar paquetes de aplicaciones usando el entorno y el apoyo del proveedor.
- *Infrastructure as a Service* (IaaS), que es el tipo más flexible para los usuarios de la nube, ya que mantienen el control de sus recursos usando la máquina virtual suministrada por el proveedor para instalar su propio sistema.

Cada uno de los usos anteriores plantea una problemática diferente, tanto en lo que se refiere a seguridad como a la hora de mejorar la autoadministración de los servicios, aspecto que constituye una de las líneas de investigación que se están desarrollando actualmente (ver [1]).

El uso de la nube, al tiempo que abre una interesante posibilidad a las empresas, plantea serias dudas respecto a

la privacidad y seguridad de los datos que éstas hayan subido a la nube. Por ello se plantea, por ejemplo, la necesidad de introducir cambios en la ciencia forense. Las empresas, especialmente las grandes, tienen sus propias políticas de seguridad y desean realizar su propia investigación, independiente de terceras partes, en caso de que ocurra un incidente.

Esto ya no es posible con el uso de la nube, y no lo es en mayor o menor grado dependiendo del tipo de servicio utilizado. En todo caso, el poder de decisión sobre la investigación a realizar en la nube ha pasado al proveedor de servicios. Se abre así una nueva líinea de investigación forense (ver [4]) que se enfrenta a nuevos retos, como es la volatilidad de datos. Además la ausencia de estándares y normativa para los procesos en la nube plantea problemas de seguridad y confianza que aún tienen que resolverse.

El hecho de que distintos recursos compartan un mismo entorno modifica la arquitectura de seguridad tradicional y abre nuevas vias de ataque. La complejidad del sistema y de la red hace prácticamente inviable el mantenimiento de una seguridad manual a cargo de administradores humanos. Sigue habiendo todo un campo de trabajo para garantizar el aislamiento tanto a nivel de computación como de redes [16]. Aparecen potenciales ataques por un usuario que elige una ubicación próxima al objetivo y realiza ataques al canal aprovechando una "mala aleatoriedad" del servidor en la nube [13].

Los problemas de seguridad que se plantean, por ejemplo, en centros virtuales de datos son diferentes de los que aparecen en recursos virtuales de telecomunicaciones en la nube suministrados por diferentes operadores [2].

Hay también importantes problemas en relación con la integridad de los datos almacenados en la red. Se pueden encontrar diferentes propuestas para resolver problemas planteados en este contexto. Por ejemplo, podemos considerar un grupo de clientes que se fían unos de otros, pero no se comunican entre ellos, y que usan los servicios de la nube suministrados por un proveedor en el que no confían totalmente. En [5] se presenta un protocolo que permite verificar la integridad de los datos almacenados, la corrección de los procesos de computación y la consistencia de la respuesta del proveedor.

En [3] se suministran los primeros esquemas que prueban la integridad y la accesibilidad de los datos almacenados en la nube. La propuesta se basa en agregar códigos de autenticación de mensaje (MACs = *Message Authentication Codes*) y enviar bloques de un archivo. La idea es obligar al "almacenista" a realizar ciertas computaciones en los bloques del fichero y comprobarlas mediante etiquetas de autenticación (tags). Las tags utilizadas en esta propuesta se basan en el RSA.

En [10] se proponen soluciones para restaurar la transparencia de la nube y conseguir mayor seguridad. Si queremos asegurar que nuestros ficheros están recuperables cuando los necesitemos (sin bajarlos periódicamente para comprobar) se pueden usar las denominadas *pruebas de recuperación* (PRs). Con los MACs se puede detectar si una parte importante de los datos ha sido borrada o dañada, pero no si ha ocurrido a pequeña escala. Se usa teoría de códigos correctores de errores para "amplificar" los errores en el fichero almacenado, pudiendo detectar cualquier corrupción en el mismo.

En [12] se plantea usar Criptografía basada en predicados, pairings y técnicas de compartición de secretos para lograr un almacenamiento privado y recuperable en la nube.

Métodos de compartición de secretos y de computación multiparte se usan también en [11] dónde se diseña un protocolo que asegura a un cliente que utiliza un *cluster* con n máquinas que un adversario no puede recuperar la información de entrada o de salida, incluso si consigue corromper a $n-1$ máquinas.

La criptografía homomórfica se perfila como una herramienta particularmente apropiada para su utilización en la red. Sin embargo, el uso de los esquemas actuales es muy costoso computacionalmente.

La noción de esquema de cifrado completamente homomórfico (*fully homomorphic encryption scheme*) fue introducida por Rivest, Adleman and Dertozous [14] poco después de la invención del RSA, inspirándose en la propiedad multiplicativa del cifrado "RSA académico": si c_1 es el cifrado de un mensaje m_1 y c_2 es el cifrado de m_2, entonces c_1c_2 es un cifrado de m_1m_2.

Rivest, Adleman y Dertouzos lo denotaron "homomorfismo de privacidad" y propusieron varios esquemas candidatos que fueron rotos poco después.

La primera propuesta de cifrado homomórfico semánticamente seguro (de acuerdo con la defición de Goldwasser y Micali [9]) aparece en la tesis doctoral de Craig Gentry [7], realizada bajo la dirección de Dan Boneh. Dados textos cifrados que cifran $\pi_1, \ldots, \pi_t$ un cifrado homomórfico permitiría generar un texto cifrado de $f(\pi_1, \ldots, \pi_t)$ para toda función f eficientemente computable. No se debería filtrar ninguna información sobre $\pi_1, \ldots, \pi_t, f(\pi_1, \ldots, \pi_t)$ o valores intermedios.

La idea de la construcción de Gentry es la siguiente:

Supongamos un esquema de cifrado con un "parámetro ruido" agregado a cada texto cifrado, de modo que la salida del algoritmo de cifrado es un texto cifrado con un pequeño ruido ($< n$), pero el algoritmo de descifrado funciona bien sólo si el ruido es menor que cierto umbral $N >> n$. Imaginemos además que existen algoritmos *Add* y *Mult* que pueden computar $E(a+b)$ y $E(a \star b)$ a partir de $E(a)$ y $E(b)$, pero a costa de sumar y multiplicar los parámetros ruido. Tenemos así un esquema de cifrado parcialmente homomórfico (*"somewhat homomorphic" encryption scheme*).

Supongamos que existe un algoritmo *Recrypt* que toma un texto cifrado $E(a)$ con ruido $N' < N$ y produce como salida un nuevo texto cifrado de a con ruido $< \sqrt{N}$. Este algoritmo

Recrypt permite construir un esquema de cifrado completamente homomórfico a partir del parcialmente homomórfico.

Conceptualmente, las técnicas utilizadas son similares a las usadas en *criptografía ayudada de servidores*, en la que un usuario con un dispositivo lento delega el trabajo de descifrado a un servidor, pero sin permitirle el descifrado total.

Para ilustrar la idea, veamos un ejemplo de juguete, debido a Gentry, que usa enteros. La llave es un entero impar $p > 2N$. Un cifrado de un bit b es un múltiplo aleatorio de p más un entero aleatorio B de la misma paridad que b: $c = b+2x+kp$ con x, k enteros aleatorios del mismo rango en $(-n/2, n/2)$.

Para descifrar se hace $b \leftarrow (a \mod p) \mod 2$. En este esquema $c \mod p$ es el parámetro ruido. Para que el descifrado funcione correctamente hace falta que $b + 2x \in [-N, N] \subset (-p/2, p/2)$.

Al sumar dos cifrados,

$$c \leftarrow c_1+c_2 = b_1+b_2+2(x_1+x_2)+(k_1+k_2)p = b_1 \oplus b_2+2x+kp.$$

El descifrado recupera $b_1 \oplus b_2$ si $(b_1 + 2x_1) + (b_2 + 2x_2) \in [-N, N]$.

Similarmente con el producto, el descifrado funciona si $(b_1 + 2x_1) \star (b_2 + 2x_2) \in [-N, N]$.

La propuesta de Gentry usa retículos de ideales y basa su seguridad en la dureza de dos problemas: un problema de decisión sobre el *caso-medio* en retículos de ideales y el *Sparse Subset Sum Problem* (SSSP).

El propio Gentry en [8] prueba una conexión entre el *caso-peor* y el *caso-medio* que permite basar su esquema en la dureza del problema del *vector independiente mas corto* (SIVP) sobre retículos de ideales en el peor caso.

En [6] los autores describen un esquema de cifrado *parcialmente homomórfico* usando sólo aritmética modular, pudiendo luego aplicar las técnicas de Gentry para convertirlo en un esquema *completamente homomórfico*.

Si bien la propuesta de Gentry representa un avance claro haciendo realidad la criptografía homomórfica, algo que para muchos parecía un utopía, el coste computacional es muy alto, inasumible todavía para un uso al nivel que se requeriría. En [15] se describen dos mejoras a la propuesta de Gentry usando un análisis mas *agresivo* del retículo de ideales y de la dureza del SSSP que les permite introducir un algoritmo de descifrado probabilístico que puede ser implementado con un circuito algebraico de bajo grado multiplicativo, lo que les lleva a conseguir un esquema de cifrado *completamente homomórfico* más rápido.

Tampoco se conoce ninguna propuesta de cifrado *completamente homomórfico* sin pasar previamente por un cifrado *parcialmente homomórfico* y la posterior aplicación del procedimiento desarrollado por Gentry, lo que abre muchas posibilidades a la investigación en el tema.

III. Cloud Computing y Seguridad

Parece fuera de dudas que el nuevo modelo de computación en la nube presenta una óptima solución para la entrega de servicios de cómputo rápidos y económicos, pero aspectos como la confidencialidad, disponibilidad e integridad de la información requieren el uso de medidas de protección, a la vista de los nuevos problemas y amenazas que han ido apareciendo.

Un aspecto clave para el éxito de la computación en la nube, es el ahorro de costes y la flexibilidad a la hora de compartir recursos y almacenamiento, redes, servidores y aplicaciones con otras organizaciones.

Pero compartir implica irremediablemente pérdida de control. Así, dependiendo del tipo de servicio contratado en la nube, muchas compañías sienten que los riesgos a los que está expuesta su información están aumentando y que sus activos críticos están más comprometidos que antes de la irrupción de la nube.

En el momento actual las compañías de todo tipo y la administración están combinando, en mayor o menor medida, servicios de *cloud computing* con infraestructuras convencionales de servicios de Tecnologías de la Información (TI). También se utilizan tanto nubes públicas como nubes privadas, tratando de lograr el mejor modelo, en términos de eficiencia y eficacia, para cada necesidad. Sin embargo, los aspectos de seguridad pueden verse afectados al no disponer de una respuesta específica, planificada con tiempo y recursos adecuados, para cubrir totalmente el problema de la seguridad en esta transición del modelo de consumo de servicios de TI.

El problema de seguridad, inherente a la migración de servicios a la nube, debería ser revisado exhaustivamente en todos sus aspectos. Es preciso asegurar la confidencialidad (que nadie pueda acceder a nuestros datos), la integridad (mis datos almacenados en la nube no pueden perderse o deteriorarse con el tiempo), e incluso la disponibilidad de nuestra información. Los recientes acontecimientos de cierre de centros de proceso de datos en la nube por distintos motivos de ámbito legal han puesto de relieve los problemas que pueden aparecer en este sentido. Hay que buscar medidas que aseguren que usuarios y organizaciones ajenas a los posibles delitos origen del cierre (pensemos en el caso Megaupload) no se vean afectadas y sin acceso a sus archivos durante un tiempo.

La implementación práctica con las tecnologías con que contamos hoy en dia, usando tanto criptografía simétrica como asimétrica, puede no ser suficiente al no haberse diseñado pensando en el contexto de la nube. Incluso parece que no se está desplegando en toda su extensión para mitigar de forma adecuada el conjunto de riesgos que han surgido y siguen surgiendo con este nuevo modelo de computación.

El ataque conocido como *man in the midle* cobra especial relevancia en este modelo y parece estar en su "mejor momento" pues la computación en la nube parece especialmente

vulnerable al mismo. Muchos de los accesos a la información que se realizan presentan vectores de ataque de este tipo.

Como clientes de servicios en la nube debemos conseguir que el control total de nuestros activos de información sea un aspecto cubierto de modo global en toda su extensión y tenga un sencillo manejo, garantizando al menos los mismos objetivos que se tenían en materia de seguridad sobre los sistemas actuales, antes de la migración a la nube. El modelo de negocio puede cambiar, pero las reglas de seguridad en ningún caso se pueden ver reducidas, todo lo contrario, deben mantenerse e incluso aumentarse con nuevas medidas que cubran los nuevos riesgos.

Son muchos los riesgos a los que están expuestos nuestros activos de información en la nube, pero podemos resumirlos en:

- **Fugas de información**. La propia naturaleza de la nube hace que sea difícil poder garantizar la trazabilidad adecuada de todos los flujos de informacion corporativa, haciendo ésta mas vulnerable por el mayor número de exposiciones (canales e intercambiadores de información) que sufre. Del mismo modo, no podemos asegurar en muchos casos el ciclo de vida de nuestros servicios: ¿Cómo se actúa en aspectos de destrucción de información cuando se dejan de utilizar los servicios de la nube? ¿Que ocurre con posibles registros intermedios utilizados por los distintos proveedores involucrados en nuestra arquitectura (copias residuales, temporales, etc.)?
- **Tecnología compartida**. De modo paralelo al nacimiento de la computación en la nube se ha ido consolidando el modelo de computación bajo virtualización: una misma máquina (servidor físico) está dividida en múltiples servidores virtuales que prestan servicio a varias compañías, distintas y heterogéneas, compartiendo el mismo hardware y sistema operativo base. Esta compartición de recursos hardware puede favorecer la explotación de una vulnerabilidad en el software utilizado para la virtualización, logrando un impacto mucho mayor que bajo entornos de computación no virtualizados. Se puede conseguir acceso a datos de múltiples compañías con un único ataque. Y se pueden plantear nuevos escenarios de riesgo en los que nuestras potenciales amenazas están compartiendo servidor físico con nosotros con la única barrera final de un software (hipervisor).
- **Usuarios internos malintencionados**. El uso de la nube eleva el nivel de riesgo en el interior de la organización, pudiendo llegarse a niveles críticos en muchos casos. El concepto de interno cambia significativamente, tanto por el elevado numero de agentes (proveedores y personal) que pueden contar con acceso a nuestra información, como por las difusas barreras entre interno y externo.
- **Perfiles desconocidos de riesgo**. La inherente falta de transparencia en la computación en la nube hace difícil cuantificar los riesgos de forma exhaustiva. No se trata sólo de un problema de cómo de seguro es un intercambiador de informacion -aspecto técnico-, sino de responsabilidades en el manejo y custodia de nuestra información, su trazabilidad y auditoría, aspectos que en la actualidad no se están cubriendo adecuadamente y que requieren una legislación específica.

Sin embargo, a pesar de los riesgos enumerados y de otros que puedan ir apareciendo ligados al modelo de la nube, las empresas están confiando en los proveedores de servicios en la nube, especialmente en aquellos que les aseguran rigor y seriedad en el tratamiento de la seguridad de la información y de los datos y una segregación adecuada de los distintos clientes en sistemas compartidos.

IV. Criptografía, la clave para la seguridad en la nube

Dentro de la industria de la seguridad hay unanimidad en que la mejor forma de proteger la información y los servicios en la nube pasa por el uso de la criptografía. No hay proveedor de servicios en la nube que no ofrezca, en su opinión, los mejores y mas avanzados estándares y técnicas criptográficas en toda su infraestructura de servicios. Así la encriptación es esencial a la hora de evitar que la información sea interpretada, en caso de ser interceptada, por personas o servicios no autorizados. Es también necesaria para proteger nuestros datos en caso de pérdida.

Del mismo modo, la criptografía proporciona un escenario óptimo para garantizar la integridad de nuestros mensajes mediante las técnicas de firma electrónica actuales, posibilitando la creación de identidades digitales, denominadas fuertes, para gestionar los accesos de usuarios, servicios y dispositivos a los datos en la nube. Permite también contar con un marco de evidencias y controles, para auditores y clientes, que garantizan su integridad con respaldo legal.

Aplicadas individual o colectivamente, parece que las técnicas actuales son válidas para cubrir gran parte de los riesgos que presenta el nuevo modelo de computación en la nube.

No obstante, no proporcionan el control global necesario sobre nuestros datos y servicios en la nube, ya que no se ha encontrado el método de encriptación, compatible con la capacidad de cómputo actual, que permita tanto el cifrado continuo y permanente de toda nuestra información como el realizar búsquedas sobre ella de forma eficiente e independientemente del lugar en que se encuentre almacenada o procesada.

Como se ha indicado, la criptografía homomórfica abre una nueva puerta, pero se hace necesario mejorar la eficiencia de modo muy sensible.

Cabe resaltar que la aplicación de la criptografía debe hacerse del modo adecuado. En otro caso se puede correr el riesgo de generar una “falsa sensación de seguridad” ya que la mera aplicación de alguna técnica, o método criptográfico no garantiza que se ha mejorado de forma real la seguridad.

Son muchos los factores a tener en cuenta y los aspectos a cuidar para una aplicación óptima y segura de la criptografía. Como ejemplo se puede citar el caso DigiNotar, emisor

de certificados de seguridad comerciales, cuya autoridad de certificación fue comprometida en agosto de 2011 por utilizar métodos criptográficamente desfasados en las funciones Hash.

Si enumeramos los niveles de aplicación práctica de la criptografía en la nube en la actualidad, las áreas de más inmediata aplicación parecen ser las siguientes:

- **Encriptación de red**. Debido a que los datos se mueven continuamente entre nubes públicas, híbridas y privadas, pudiendo considerarse la red insegura en cualquiera de estos tránsitos, todos nuestros datos deben ser cifrados en su transporte, independientemente de origen y destino.
- **Almacenamiento encriptado**. Cualquier información susceptible de ser almacenada en la nube debería ser encriptada, tanto si es un dato a largo plazo, como una caché temporal o una base de datos viva. El almacenamiento encriptado es viable en muchos casos hoy en dia, de manera relativamente fácil de implementar y transparente al usuario. Pero hay retos por resolver para lograr su plena eficiencia, que afectan tanto a la gestión de claves como a la recuperación ante una contingencia o al porcentaje de tiempo que nuestros datos no están cifrados. El impacto actual, computacionalmente hablando, de una implementación global de encriptación en este campo parece que no es viable con las técnicas actuales (RSA, etc.)
- **Integridad de datos, software y sistemas**. La garantía de que nuestros datos no han sido modificados, voluntaria o involuntariamente, maliciosamente o por accidente, cobra mayor valor en este nuevo modelo de computación. Del mismo modo, los sistemas y software que dan soporte a los servicios en la nube deben poder garantizar su autenticidad. Las técnicas actuales de firma electrónica proporcionan un método seguro y robusto para cubrir este aspecto, tanto en la integridad de mensajes como datos y sistemas, pero en ciertos contextos, con múltiples mensajes y documentos en curso, puede ser muy duro y pesado de implementar.
- **Autenticación criptográfica**. Es éste uno de los campos de mayor y mas eficiente aplicación de la criptografía en la nube. Las técnicas actuales de criptografía para la creación de identidades digitales parece ser adecuada. Se cuenta además con multiples tecnologías en este sentido (Smartcards, OTP, etc.)
- **Trazabilidad y auditoría**. El registro y posterior auditoría de eventos en la nube, sin resquicio para la duda y con pleno respaldo legal, es un aspecto crítico a tener en cuenta en el nuevo modelo de computación en la nube. Hace falta una normativa clara, que debería ser de obligado cumplimiento por todo proveedor y formar parte de los distintos acuerdos de servicios establecidos. Las técnicas de firma electrónica, sellado de tiempo, controles duales, y otras relacionadas con la criptografía actual, permiten garantizar algunos de estos aspectos, pero como se ha indicado, se ha abierto una nueva línea a la investigación forense.

V. Conclusión

Hemos tratado de presentar el nuevo escenario de la computación en la nube, mostrando que hay una actividad creciente de investigación generada por la nueva situación, adaptando herramientas y conceptos utilizados en la situación anterior (técnicas de códigos correctores, compartición de secretos, criptografía basada en atributos, seguridad semántica, criptografía de clave pública y privada, autenticación, etc.) y desarrollando herramientas específicamente diseñadas para la nube y que abren nuevas posibilidades, como la criptografía completamente homomórfica, que se muestra como una esperanzadora posibilidad, pero que requiere mejoras notables en su coste computacional. Hemos mencionado algunas de las soluciones actuales y planteado nuevas amenazas que tienen que ser tenidas en cuenta. En resumen, consideramos que la nube es una magnífica posibili-dad técnica, económica y empresarial, pero ha generado la aparición de nueva amenazas que tienen que ser consideradas seriamente para buscar soluciones que favorezcan la confianza en el uso de la nube. Al mismo tiempo, se abren nuevas y apasionantes líneas de investigación en criptografía.

Agradecimientos

Los autores agradecen la colaboración científica del grupo investigador que forma parte de la Cátedra de Inteligencia Analítica avanzada de la Universidad de Oviedo, al que pertenecen las empresas Inixa y NeoMetrics, especialmente a su responsable y director, el profesor Santos González. Asímismo agradecen a los referees sus comentarios y sugerencias.

References

[1] I. M. Abbadi, “Self-Managed Services Conceptual Models in Trushtworthy Cloud’s Infrastructure”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[2] M. Aslam and C. Gehrmann, “Security Considerations for Virtual Platform Provisioning”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[3] G. Ateniese, “The cloud was tipsy and ate my files!”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[4] D. Birk, “Technical Challenges of Forensic Investigations in Cloud Computing Environments”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[5] C. Cachim, “Integrity and Consistency for Untrusted Services”, en *P*roc.” Workshop on Cryptography and Security in Clouds, Zurich 2011.

[6] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, “Fully Homomorphic Encryption onve the Integers”, en *E*urocrypt 2010, 2010.

[7] C. Gentry, “A Fully Homomorphic Encryption Scheme ”, PhD. Disertation, Stanford University, 2009.

[8] C. Gentry, “Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness”, en *C*rypto 2010, LNCS 6223, pp.116-137, 2010.

[9] S. Goldwasser and S. Micali, “Probabilistic encryption and how to play mental poker keeping secret all partial information”, en *P*roc of STOC ’82, pp. 365–377, 1982

[10] A. Juels, “Writting on Wind and Water: Storage Security in the Cloud”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[11] S. Kamara and M. Raykova, “Secure Outsourced Computation in a Multi-tenant Cloud”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[12] G. Persiano, “Predicate Encryption for Private and Serchable Remote Storage”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.

[13] T. Ristenpart, “Virtual Security: Information Leakage in Clouds and VM Reset Vulnearabilities”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.
[14] R. Rivest, L. Adleman, and M. Dertouzos, “On data banks and privacy homomorphisms”, en *F*oundations of Secure Computation, pp. 169–180, 1978.
[15] D. Stehle and R. Steinfeld, “Faster Fully Homomorphic Encryption”, en emph Asiacrypt 2010, LNCS 6477, pp. 377-394, 2010.
[16] A. Waily, M. Lacoste and H.Devar, “Towars Multi-Layers Autonomic Isolation of Cloud Computing and Networking Resources”, en *P*roc. Workshop on Cryptography and Security in Clouds, Zurich 2011.