Comunicación Entre Ordenadores y la Cloud Computing

Elio Rodo Terrazas Bustamante
Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Informática
Simulación de Sistemas
elioterrazas@hotmail.com

RESUMEN

En este artículo describiremos de manera básica lo que es Cloud Computing, a su vez explicaremos algunos factores de seguridad novedosos e importantes que son tomados en cuenta en este nuevo paradigma por los proveedores de servicios en la nube, para la seguridad de los datos de los clientes en las comunicaciones y la manipulación de su información, y daremos una idea de la proyección que tienen las comunicaciones entre ordenadores en un futuro no muy lejano, cuando sea algo natural hablar de Cloud Computing.

Palabras Clave

Comunicación, Computación en la nube, HTTPS, SSL, TSL.

1. INTRODUCCIÓN

El Internet es actualmente uno de los medios de comunicación más importantes y utilizados del mundo, personas y organizaciones lo utilizan para obtener, compartir y enviar información de cualquier tipo, lamentablemente la existencia de virus informáticos, espías, troyanos, ataques de hackers y otros tipos de males atentan contra la integridad de dicha información, aumentando así la necesidad de resguardarla por ser fundamental para estas organizaciones y/o personas, por esta razón es que día a día adquieren programas o equipos que permitan asegurar su información, como ser antivirus, antispam, firewalls, IPS, etc., y por esto se debía tener una visión esencialmente centrada tipo CAPEX (costos de capital)[2], esto significa que la Empresa debía pensar en destinar un capital importante en adquirir desde computadoras personales hasta toda una infraestructura computacional compleja altamente costosa para implementar las TIC necesarias, además de actualizarla cuando sea pertinente, comprar licencias, antivirus y otros, y contratar el personal que opere estos recursos; Convirtiéndose así en una barrera para el crecimiento de la organización; ahora con la llegada del paradigma computacional "Computación en la Nube (Cloud Computing)" que si no elimina totalmente el problema, al menos lo minimiza de gran manera, ofreciendo todos estos recursos anteriormente mencionados, además de otorgar la seguridad que estas requieran para la manipulación de su información y sus "Comunicaciones entre Ordenadores" o usuarios de su red corporativa, todo esto pagando solamente el flete de uso de estos servicios.

2. LA COMUNICACIÓN EN LA NUBE

2.1 ¿Qué es la computación en la nube?

"Cloud Computing o Computación en la Nube, es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado" [1].

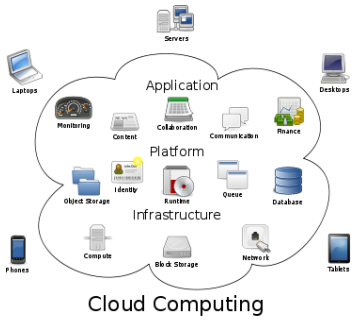

Figura 1. La Computación en la Nube.

Esto significa que la Computación en la Nube básicamente es un modelo computacional, donde los usuarios obtienen servicios según sus necesidades, ya sean empresariales u otras, de un conjunto de recursos computacionales que ofrecen en la actualidad varios proveedores como Microsoft, Salesforce, Google Apps, etc., estos recursos podrían consistir en: CPU, Disco Duro, Capacidades de transferencia en red, seguridad bajo demanda, optimización de aplicaciones, etc. Que cuando ya no se los requieran estos sencillamente se los deje de usar y/o desalojar, en la Figura 1 podemos ver una idea de los servicios dados.

2.2 Servicios y forma de acceso a la Nube

Como se mencionó anteriormente que la Computación en la Nube es la obtención de servicios bajo demanda de un conjunto de recursos como ser CPU, RAM, Disco Duro, Aplicaciones, esto significa que un usuario cualquiera podrá acceder al uso de estos recursos con tan solo una computadora, celular, i-pad, u otro dispositivo que tenga acceso a internet además de tener algún navegador instalado, para que de esta forma el usuario acceda a la página del proveedor de servicios, ingrese a su cuenta y acceda así al uso de los recursos alquilados de dicho proveedor en la nube, el usuario tendrá la opción de activar la "conexión segura (HTTPS)", un ejemplo podría ser el servicio gratuito de SkyDrive que a usuarios registrados les brinda de manera gratuita 26 Gb. de espacio de almacenamiento, además de un pool de aplicaciones de Office básico, el cual está disponible para la edición de documentos Word, Excel, Power Point, etc., los cuales a su vez se podrán almacenar en la PC Virtual de la nube para luego poder acceder a ellos desde cualquier parte del planeta.

2.3 Conexiones y comunicación con la Nube

Los usuarios de estos servicios en la nube, ya sean personas u organizaciones, deben tener una comunicación segura con los proveedores, para evitar la interferencia o el robo de información del usuario, por lo que la Cloud Computing utiliza de forma casi estándar el protocolo encriptado de Internet (HTTPS) para estas conexiones. A continuación explicaremos los protocolos más utilizados en la Cloud Computing.

2.3.1 Protocolo HTTPS

"Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP" [3]. Este protocolo a diferencia del http simple, encripta la información bajo el cifrado SSL o TSL, esto significa que permite tener una conexión más segura para evitar así los ataques conocidos como Man-In-The-Midle(Hombre en el Medio), ya que este tipo de ataques consisten básicamente en interferir la tubería de información y así efectuar escuchas, manipulación y/o forjado de información.

Sintácticamente, los mensajes HTTPS son los mismos como HTTP, que consisten en una línea de petición o de estado seguido de encabezados y un cuerpo [4], la diferencia es que HTTPS adiciona una orden de uso de capa adicional de encriptación SSL o TSL, esto hace que todo el mensaje HTTPS este cifrado, incluyendo cabeceras y la solicitud o respuesta, con la excepción de las direcciones IP y números de puerto que no se pueden cifrar, ya que estos son propios de la comunicación TCP-IP.

Por ultimo mencionar que para mayor seguridad a la hora de utilizar HTTPS "Un sitio debe estar completamente organizado a través de HTTPS, sin tener parte de su contenido cargado a través de HTTP" [3], por que debido a esto es que se podría producir los denominados ataques de vigilancia.

2.3.2 Protocolo SSL y TSL

"Secure Sockets Layer (SSL; en español «capa de conexión segura») y su sucesor Transport Layer Security (TLS; en español «seguridad de la capa de transporte») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet" [4]. La manera de trabajo de estos es que SSL y TLS cifran los segmentos de conexiones de red en la capa de aplicación para la capa de transporte, utilizando criptografía asimétrica para el intercambio de claves, cifrado simétrico de confidencialidad, y los códigos de autenticación de mensajes para la integridad del mensaje.

El uso de SSL y TSL son no solamente con el HTTPS sino que son utilizados para la encapsulación de diferentes protocolos de nivel superior, con el fin de crear conexiones más seguras.

Estos protocolos tienen tres características importantes que son:

La conexión es privada. El cifrado se utiliza después de un primer encuentro en el que se define una clave secreta. La criptografía simétrica se utiliza para el cifrado de datos (por ejemplo, DES - DES, 3DES - 3DES, RC4 - SCH).

La identidad del otro extremo se puede autenticar utilizando asimetría o clave pública, cifrado (por ejemplo, RSA o DSS).

La conexión es fiable. El mensaje de transporte incluye un mensaje de comprobación de integridad mediante una llave "Message Authentication Code (MAC)" [5]. Las funciones de hash seguras (por ejemplo, SHA, MD5) se utilizan para calcular el MAC.

Luego de que la conexión está establecida el cliente y el servidor utilizan las claves de sesión para cifrar y descifrar los datos que se envían entre sí y también para validar su integridad, cada lado puede renegociar la conexión, en cuyo caso, el proceso se repite a sí mismo, si no pasa esto, todo continua hasta que se cierra la conexión. Si cualquier paso fallara, el protocolo de enlace TLS/SSL falla y la conexión no se creara.

2.4 Problemática actual de la Comunicación Interna Virtual en la Nube

El solo concepto de virtualización en servidores, obliga a replantear muchos temas de seguridad, uno de los grandes preceptos es que el administrador IT debe tener la visibilidad del tráfico que existe en el centro de datos entre los servidores físicos, esa visibilidad ya no está garantizada cuando nos movemos a servicios virtuales, ya que no importaría que tengamos Firewalls o IPS's en la red, cuando el tráfico es inter-máquina virtual (nunca se sale del servidor físico),por tanto ¿qué consideraciones se debería tener?, ¿qué inteligencia se debería llevar hacia adentro del servidor físico para no perder esta telemetría y esta visibilidad de los diferentes flujos que ocurren entre máquinas virtuales dentro de un mismo servidor físico, o en un modelo multi-tenancy en el que se debe tener en cuenta la seguridad?; esta es la problemática actual que grandes empresas como Cisco, Microsoft y otros están tratando de resolver.

3. CONCLUSIONES

1. La nueva visión OPEX (costos operativos) en las organizaciones, facilita de gran manera la adquisición de infraestructura y TIC's necesarias para estas, dando la oportunidad de ahorrar y reinvertir todos esos recursos.

2. La idea de usar Escritorio Virtual, es muy positiva porque resuelve el problema de una posible brecha de seguridad en el dispositivo del usuario que pueda amenazar la integridad de los sistemas, o la información de la Empresa u Organización.

3. Con la Cloud Computing la seguridad deja de ser solamente Perimetral, añadiendo una problemática más compleja de inter-máquina virtual, que aún se encuentra en discusión.

4. REFERENCIAS

[1] Computación en la Nube, http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube#cite_note-0, 04 octubre 2012.

[2] De Logicalis now – Seguridad informática en tiempos de Cloud Computing, http://www.la.logicalis.com/pdf/2011-02-11-Entrega18-Logicalis%20Now%20N%C2%BA13.pdf, Marzo 2011.

[3] Hypertext Transfer Protocol Secure http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure, 11 octubre 2012.

[4] Transport Layer Security - http://es.wikipedia.org/wiki/Transport_Layer_Security, 13 septiembre 2012.

[5] The Secure Sockets Layer (SSL) Protocol Version 3.0 - http://tools.ietf.org/html/rfc6101, agosto 2011.