THE CLOUD
UN NUEVO PARADIGMA

Por Rody Joshua Carbajal

Universidad de Ceutec Honduras

Noviembre 2015

INDICE

Introduccion_____3

¿Qué es la nube? _____4

¿Cuál es la tendencia? _____5

Vulnerabilidades en la nube_____10

Computación Cuantica_____13

Conclusion_____16

Everyone use the term cloud, usually use to refer a place that stored things, but do they really know what is?

Cloud computing goes beyond that, in this paper is known as the new paradigm of computing, and we are going to talk about how is molding a new era in computer science, how is going to change the way we use internet, and more important yet,

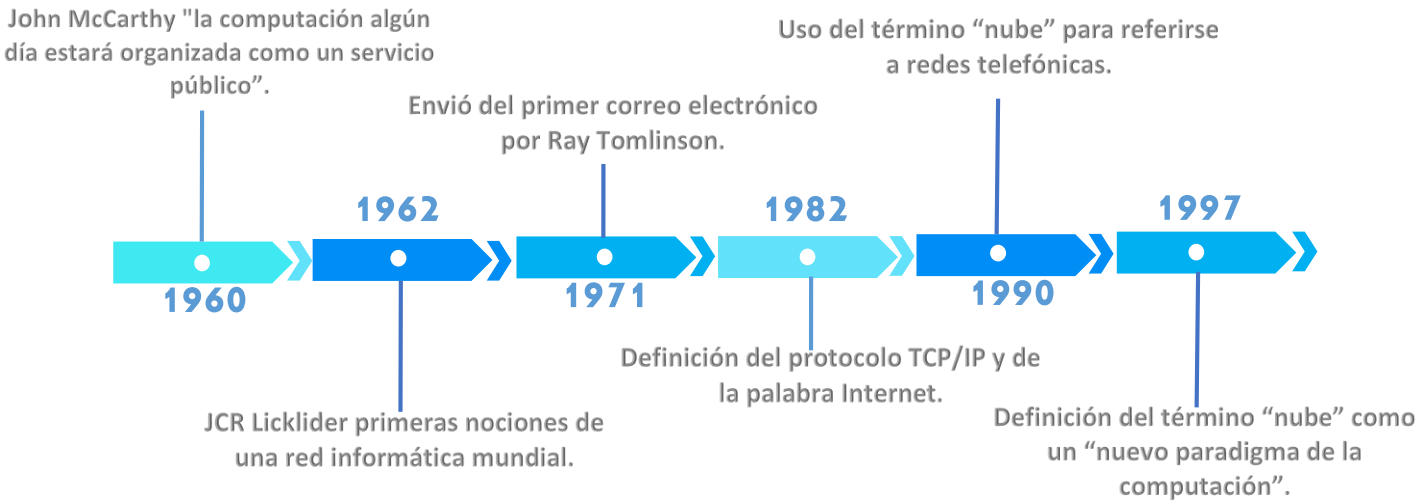
how secure is the cloud? what are their vulnerabilities? and how we can address them.

INTRODUCCION

Al hablar de la nube es indispensable hacer mención de dos importantes figuras dentro del ámbito informático, John McCarthy prominente científico de la computación quien dijo,

" La computación algún día estará organizada como un servicio público" y JCR Licklider informático teórico, precursor de lo que actualmente es el internet gracias a sus aportes en redes globales, ambos con sus respectivas premoniciones hicieron posible la computación en la nube.

En 1962 después de ser nombrado jefe de la oficina de procesado de información, Licklider empieza a formar un grupo dentro de DARPA para investigaciones de ordenadores más avanzados. Como parte esencial para sus investigaciones se instalan tres terminales de redes en distintas locaciones una en santa Mónica la S.D.C, otra en la universidad de California(Berkeley) y la ultima en el instituto tecnológico de Massachusetts, subsiguiente a la instalación de la terminales surge el problema en la interactividad, cada una de las tres terminales tenían diferentes comandos de usuario, que inhabilitaban la comunicación con las otras terminales así que si deseaba hablar con otra terminal tenía que movilizarse y registrase en esa terminal. Es ahí donde se concebí la noción de ARPANet y lo que sería la evolución de la comunicación y la trasferencia de información. El ARPANet fue una red de Computadoras que se comunicaba a través de protocolos(un protocolo es un lenguaje que utilizan las computadoras al compartir recursos) el ARPNet es sus inicios utilizaba el protocolo NCP(Programa de control de red) para establecer la conexión, pero su expansión fue de una forma exponencial que dio origen al protocolo de comunicación TCP/IP(Protocolo de control de transmisión), protocolo que se convertiría en el lenguaje común para las intercomunicaciones y el que permitiría la transición de ARPnet a la red de redes llamada "Internet" la base de la computación en la nube.



¿Qué es la nube?

Se puede definir como una Interconectividad de redes con la extensión de servicios y aplicaciones en todo momento a través de una conexión a internet.

Un perfecto ejemplo para comprender la nube puede ser el lanzamiento de google docs. en 2006, que es además el punto donde se llega a materializar el concepto abstracto de la computación en la nube en lo que conocemos en la actualidad.

¿Cómo se llega a materializar?

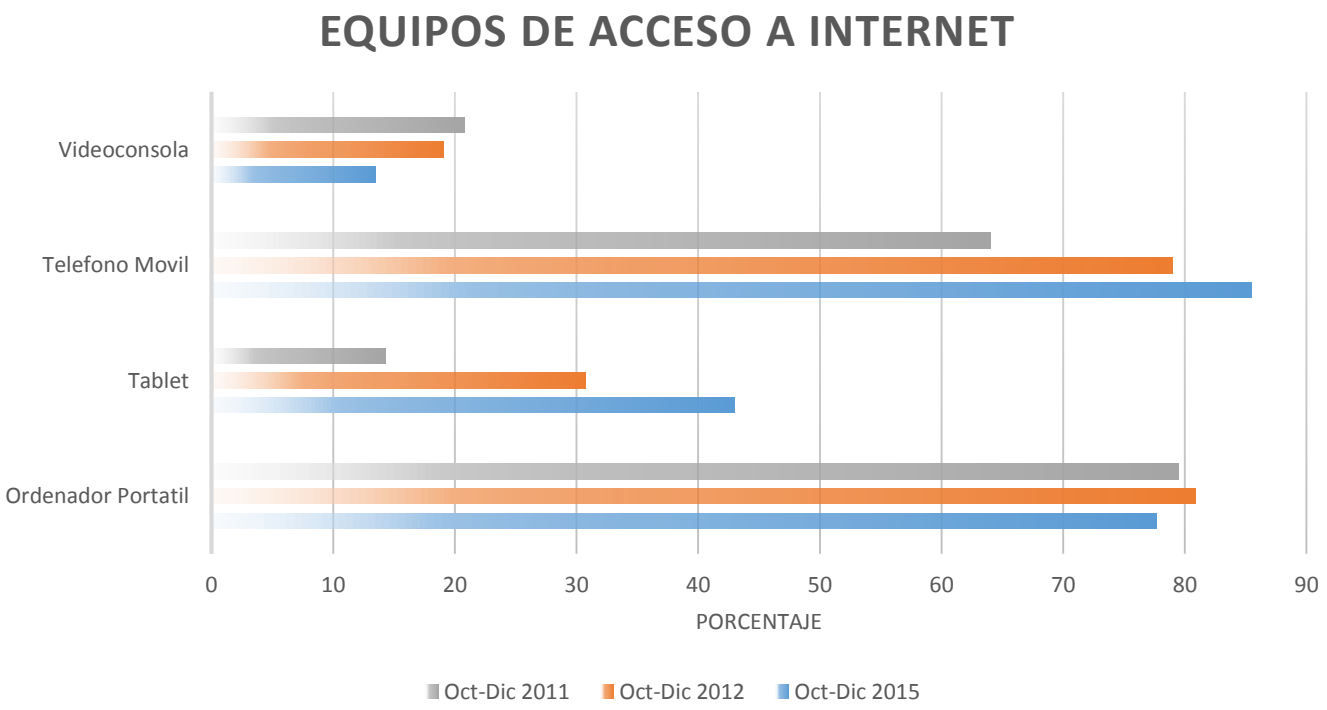
Google docs provee la facilidad de comunicación entre ordenadores, se observa la premonición de una red global y descentralizada hecha realidad, pero además del servicio de comunicación, ofrece la posibilidad de acceder a aplicaciones, la facilidad de trabajo en conjunto además de almacenamiento y recuperación de datos en cualquier momento, es muy sencillo observar una evolución en la computación, se puede ver la informática en la nube tomado su forma.

Gracias a la nube se puede hacer uso de aplicaciones sin necesidad de instalarlas en el ordenador, se resuelve el problema de espacio en memoria, la tendencia se convierte en más software menos hardware, además te permite almacenar múltiples datos de interés y tener acceso a ellos en cualquier instante, esas entre muchas otras funciones conforman la nube, pero talvez la más trascendental de todas sea la compatibilidad con diferentes dispositivos.

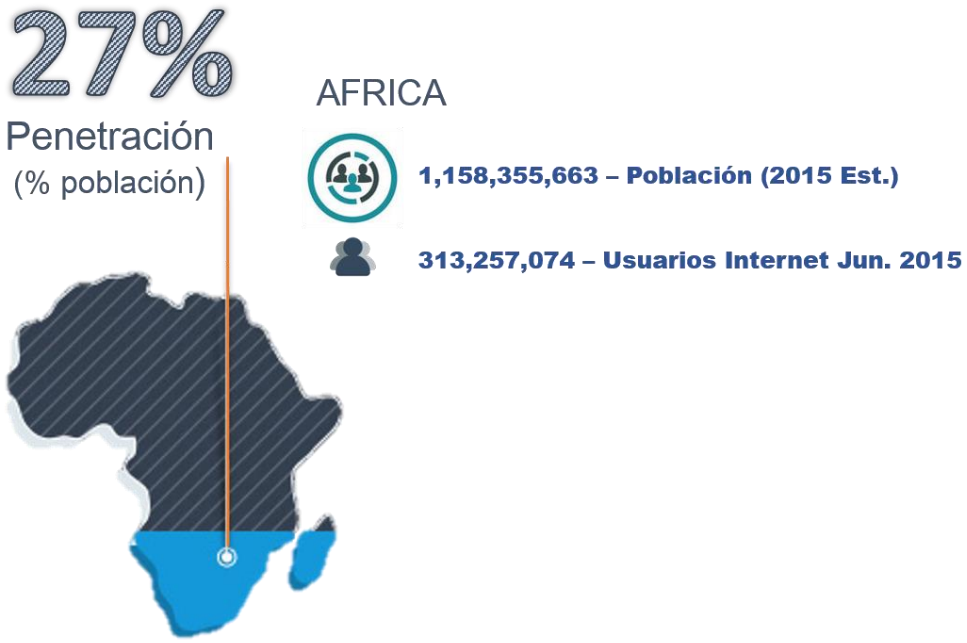
Siendo menos técnico es

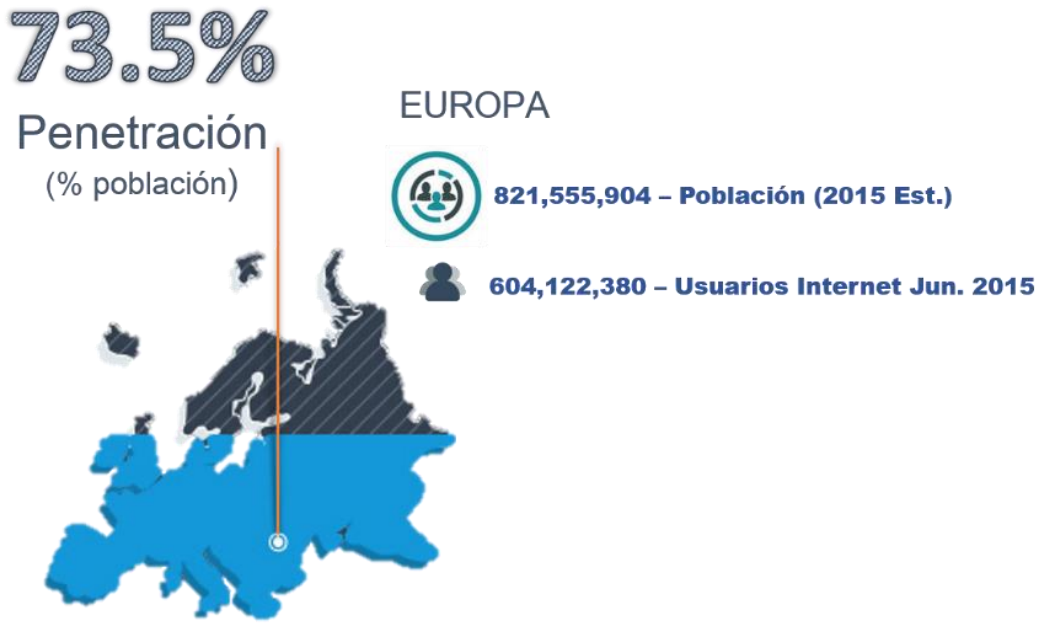
¿Cuál es la tendencia?

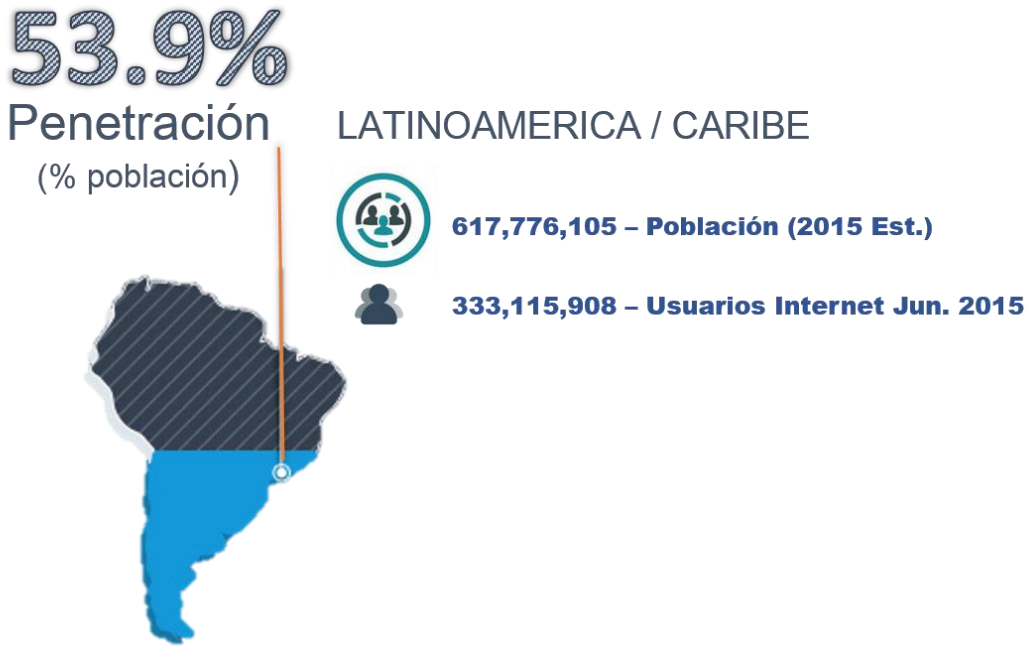
Computadoras personales por cada 100 personas para el año 2006 en estados unidos era de un 80.61 por ciento, porcentaje que ha incrementado de forma exponencial en los últimos años, además la llegada de los Smartphones y tablets ha permitido que estemos aún más conectados. Aquí se muestra un gráfico haciendo énfasis en el crecimiento de los teléfonos inteligentes o Smartphones como modo de acceso habitual al internet.



Otra estadística de relevancia e importante de hacer mención es el acceso a internet. En las siguientes infografías podremos visualizar el porcentaje de penetración de internet en ciertos continentes y regiones como además una estimación del número de población y sus usuarios activos para el año 2015.







Tenemos subsecuentemente que el país con mayor porcentaje en penetración de internet en los últimos años a Norte América y al continente africano con el porcentaje mas bajo.

¿Que nos indican estos gráficos?

En los gráficos anteriores mostramos la tendencia actual de la nube, el primer grafico siendo el incremento en el uso de smartphones como la herramienta principal para conectarse a la red y los siguientes gráficos indicando el porcentaje de penetración de internet por regiones y por países.

Adicionalmente haremos mención de dos proyectos a implementar para el año 2016. El primer proyecto es desarrollado por Facebook, la compañía llego a un acuerdo con Eutelsat empresa francesa dueña de 38 satélites de comunicaciones, para proveer internet gratis al continente africano a inicios del 2016. Eutelsat asegura que su tecnología hará posible que los usuarios incluso en los lugares más remotos del continente africano pueden llegar a conectarse a la red.

El siguiente proyecto es llamado loon, creado por google, la idea es cubrir por completo al mundo de una red de globos que viajaran en la estratosfera a 20 km de la superficie terrestre superado dos veces la altura de los aviones y del clima, google asegura que la estructura del globo y los componentes de alta calidad, lo mantendrán flotando en la estratosfera por 100 días además al momento de retíralo de servicio las múltiples métricas de seguridad aseguran que su descenso será de forma controlada.

"Cada globo puede proporcionar conectividad a un área terrestre de aproximadamente 40 km de diámetro mediante una tecnología de comunicación inalámbrica llamada LTE.

Para usar LTE, el Proyecto Loon se asocia con empresas de telecomunicación para compartir el espectro celular, de manera que las personas puedan acceder a Internet desde cualquier lugar directamente con sus teléfonos y otros dispositivos habilitados para LTE. Los globos transmiten el tráfico inalámbrico de teléfonos celulares y otros dispositivos a la Internet global mediante vínculos de alta velocidad."

Información proporcionada por http://www.google.com/intl/es-419/loon/how/

Encontramos que la tendencia es una comunidad global conectada en todo momento al internet cada vez siendo de preferencia los Smartphones como herramienta habitual.

Significa la nube en todo momento y en cualquier lugar del mundo sin ningún limitante.

Tal ha sido el crecimiento de la nube que se origina el primer teléfono inteligente basado en esa tecnología, llamado robin, creado por la compañía nextbit, un teléfono con memoria ilimitada asegura la compañía, el Smartphone ofrece 100gb de almacenamiento en la nube sin costo alguno, más la opción de poder obtener más espacio según sea la necesidad del cliente. El robin ofrece funciones únicas en cuanto a la gestión de contenido y almacenamiento, por instancia el teléfono reconoce y analiza las aplicaciones menos usadas en el teléfono, e inmediatamente las transfiere a la nube despejando memoria en el dispositivo, esa innovadora función además de la gestión automática de música, imágenes, videos u otros archivos de importancia hacen crecer cada día mas la computación en la nube.

nextbit

Hemos estado haciendo énfasis en una conectividad ininterrumpida que ofrece el internet ya que la computación en la nube y la red de redes están íntimamente relacionadas, es más, la única limitante de la computación en la nube es el internet no se podrían brindar los servicios que ofrece la nube sin una conexión a la red, pero gracias a las brillantes innovaciones para abordar esa limitante, la nube parece cada día estar más consolidada en todo el globo.

Ya hemos definido como se origina la nube, que ofrece esa nueva tecnología además de su tendencia actual, pero haciendo uso del internet como principal vía, cuales son, los riesgos a mi privacidad, a mi información personal ¿se podría llegar a comprometer la integridad de mi equipo? ¿Si es así como?

Llegamos al punto donde debemos abordar las existentes vulnerabilidades de la computación en la nube.

- El acceso no autorizado a datos
- Phishing
- Interceptación de correos electrónicos.

Vulnerabilidades en la nube

Una de las vulnerabilidades mas fuertes en la nube es la sincronía de datos a través de dispositivos, si a su vez brinda múltiples beneficios también esta la gran desventaja del acceso no autorizado a datos. se podría dar el caso de la adquisición ilegal de una cuenta para tener total acceso a la información que reside en el servidor o nube y ya que más de un dispositivo esta anclado al servicio, la filtración de información seria a gran escala. Un excelente ejemplo se da en el servicio ofrecido por apple llamado icloud, servicio que mantiene en sincronía todos los dispositivos Apple que la persona posea, así si se llegara a encontrar una vulnerabilidad en el sistema como en el caso que se dio de la filtración de imágenes privadas de celebridades, vulnerabilidad explotada, mas el nivel bajo de seguridad en las contraseñas, hicieron posible que un programa de fuerza bruta, probara permutaciones y combinaciones de contraseñas hasta encontrar la correcta y de esa forma filtrar contenido delicado de cada usuario. No solo la violación de privacidad esta juego aquí, muchas veces se utilizan métodos de acceso no autorizado a datos para extorsionar a las personas, es donde entra el termino phishing, termino en informática que se utiliza cuando una persona denominada phisher intenta de forma fraudulenta adquirir información confidencial, haciéndose pasar por una persona o empresa de confianza.

Intercepción de datos

Otra vulnerabilidad es la intercepción de correos electrónicos entre otros datos, El interceptar la correspondencia electrónica puede servir no sólo para obtener información privada , sino también para modificar o falsificar un cheque electrónico. El programa que se utiliza es llamado sniffer, aplicación especial que permite capturar paquetes que viajan por la red, como por ejemplo leer un correo de Hotmail. El usuario da su login y clave, datos que viajan al fichero de password del sistema y en donde el sniffer actúa interceptando los datos para después guardarlos en un fichero para su posterior uso.

¿Cual es la relación con la nube? El servicio en la nube solicita algún tipo de autenticación por lo general se hace a través de un correo electrónico, por eso la lógica permanece la misma, al momento de vulnerar información a través de sniffing.

Perdida de datos

La siguiente vulnerabilidad es la perdida de datos, puede ocurrir cuando una unidad de disco duro muere y la persona encargada de hacer respaldos no lo hace para esa unidad, otro escenario es cuando el propietario de los datos cifrados pierde la llave de acceso y el ultimo se da cuando intencionalmente se hace una ataque malicioso a los servidores.

Siguiendo el escenario de ataques deliberados tenemos el sqli, inyección de código en la consulta, es una técnica para modificar cadenas de consultas de base de datos. La intrusión ocurre durante la ejecución del programa vulnerable, ya sea, en computadores de escritorio o bien en sitios Web, en este último caso obviamente ejecutándose en el servidor que los aloja. Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar otro tipo de código malicioso en el computador.

Tenemos otro de los ataques más populares a los servidores llamado DoS (ataques de denegación de servicio), funcionan cuando una computadora con una conexión a Internet intenta inundar un servidor con paquetes. Consiste básicamente en enviar un gran número de peticiones a un servidor de manera que los usuarios legítimos del servicio no puedan acceder a esos recursos.

Uno de los malware más peligrosos, desplegados en servidores es el de tipo ransomware como el Linux.Encoder 1 el cual cifrara directorios y/o archivos y pedirá rescate por ellos, es importante hacer mención que este nuevo tipo de malware podría cifrar hasta directorios de backup, dejándonos con pocas opciones de recuperar nuestra información. La opción que jamás debemos considerar es la del pago por rescate, ya que no habrá ninguna garantía de la integridad de mis archivos al momento de retornarlos, además de posibles chantajes.

Recordemos que la nube es una metáfora, la nube son múltiples servidores alojados en inmensas instalaciones conectadas a la red, en consecuencia hemos descrito las principales vulnerabilidades en la nube.

Computación Cuántica

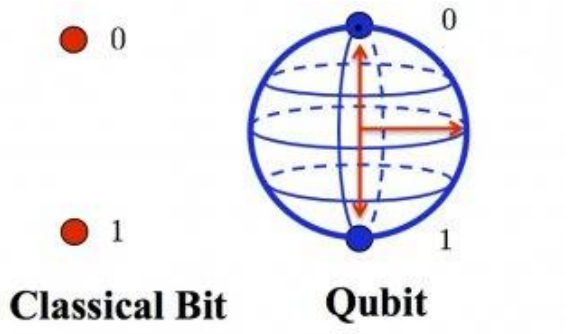
Una innovadora opción para contrarrestar estas vulnerabilidades es la computación cuántica, es cierto que es una tecnología que apenas se esta empezando a explorar y comprender, pero este año se puede decir que se ha dado el primer paso, google y la nasa adquieren la supercomputadora cuántica creada por la compañía Dwave system, adquisición que abre un sinnúmero de aplicaciones en el ámbito informático, para hacer mención de algunas de sus aplicaciones están los problemas de optimización resueltos en segundos, inteligencia artificial, maquinas capaces de reconocer objetos a través de una detección de patrones recurrentes la cual también forma parte de un problema de optimización, ya que la cantidad de variables, datos y algoritmos que se introducen mas el inmenso numero de combinaciones potenciales de datos, hacen tal tarea de alto costo computacional, estas y muchas otras aplicaciones ofrece la computación cuántica, pero referente a las vulnerabilidades previamente mencionadas tenemos la criptografía cuántica para ser mas específicos la distribución de llave cuántica QKD, hablábamos que unos de los mayores problemas en la nube es la intercepción de datos por terceros, o espías, siendo ellos capaces de adquirir información delicada como nuestro numero de cuentas, correos electrónicos, hasta las contraseñas de nuestras cuentas, todo tipo de dato que hace posible la filtración de información privada que tengamos almacenada en la nube, es aquí donde entra la distribución de llave cuántica, la cual hace uso de leyes de la física cuántica para asegurar nuestra información.

D-Wave
The Quantum Computing Company™

¿Cómo funciona?

Describiremos dos términos propios de la física cuántica que fueron llevados y/o implementados con éxito en la computación.

Primero tenemos la superposición cuántica, ocurre cuando un objeto posee simultáneamente dos o mas valores de una cantidad observable, en la supercomputadora Dwave, significa que la computadora hace posible que los 1 y 0 sean simultáneamente uno solo, en la Dwave se conocen como qubits, significa que la computadora considera y manipula todas las combinaciones de bits simultáneamente, haciendo la computación cuántica rápida y potente.



El siguiente termino es entrelazamiento cuántico, En términos sencillos, el entrelazamiento cuántico se produce cuando partículas tales como fotones y electrones interactúan físicamente para después separarse sin dejar de conservar una conexión estrecha. Un aspecto relacionado y crucial de cara a aplicaciones de comunicación es que, dado que los pares de fotones poseen un vínculo intrínseco, ofrecen seguridad, ya que si se mide un fotón, revelará con completa certeza lo mismo que revelaría el otro fotón si fuera medido. Asimismo, si la señal fuera interceptada por un tercero, esto sería detectado de manera inmediata, puesto que para interceptar el mensaje habría que desbaratar el entrelazamiento. Y una vez se rompe este, no se puede recuperar.

Teniendo conocimiento de estos dos términos, y su implementación en la informática, la distribución de llave cuántica de esa forma trabaja, los datos encriptados se trasmiten a través de la red, pero la llave para des encriptar los datos se trasmiten por separado, la llave aleatoria que es generado por un motor cuántico transmite la llave en forma de fotones por un fibra óptica especial, la cual haciendo uso de la leyes de la física cuántica hace imposible el robo o la intercepción de misma llave, ya que si se llegara a intentar interceptar o modificar la llave que viaja por la fibra óptica, alertaría al sistema de un intento de entrada no autorizada, eso se llama el efecto de entrelazamiento cuántico o como Einstein la llamaba una espeluznante acción a distancia.

Datos encriptados viajando por la red.

Llave generada de forma aleatoria en el motor cuántico viajando como fotón

Imágenes proporcionadas por battelleInnovations.

Conclusión

Es cierto que algunas vulnerabilidades las podemos evitar siendo más consiente de los riegos de la red, pero hay otras que están fuera de nuestro alcance, y en esta última debemos confiar en las métricas de seguridad de cada compañía para la protección de nuestra información.

La tecnología cuántica recién está en su estado de infancia, pero esperamos que algún día, mas ahora con el crecimiento exponencial de la tecnología, se convierta en una parte intrínseca en la seguridad computacional.

¿Será que la computación cuántica resolverá las vulnerabilidades de la nube en un futuro cercano?

Bibliografía

https://es.wikipedia.org/wiki/Historia_de_Internet

http://www.computacionennube.org/computacion-en-nube/

http://stats.wikiprogress.org/Index.aspx?DataSetCode=PERSONALCOMPUTERS

http://www.exitoexportador.com/stats.htm

http://www.google.com/intl/es-419/loon/how/

http://cordis.europa.eu/result/rcn/91667_es.html

http://www.dwavesys.com/quantum-computing

https://en.wikipedia.org/wiki/Linux.Encoder.1

http://www.lanacion.com.ar/1824138-nexbit-robin-el-teletono-movil-con-almacenamiento-ilimitado