Polo del Conocimiento

Pol. Con. (Edición núm. 19) Vol. 3, No 5
Mayo 2018, pp. 260-279
ISSN: 2550 - 682X
DOI: 10.23857/pc.v3i5.640

Recepción: 07 / 02 / 2018
Aceptación: 15 / 04 / 2018
Publicación: 08 / 05 / 2018



Ciencias de la Computación
Artículo de Revisión

# Tendencias tecnológicas y desafíos de la seguridad informática

## *Technological Trends and Challenges of Computer Security*

## *Tendências Tecnológicas e Desafios da Segurança Informática*

Carlos J. Martínez-Santander [I]
cmartinezs@ucacue.edu.ec

Yolanda de la N. Cruz-Gavilánez [II]
nube5502@gmail.com

**Correspondencia:** cmartinezs@ucacue.edu.ec

[I] Docente, Universidad Católica de Cuenca, Azuay, Ecuador.

[II] Docente, Universidad Católica de Cuenca, Azuay, Ecuador.

## Resumen

En la última década tecnologías como Internet de las cosas, Computación en la nube, Bitcoin, han ganado popularidad debido a los desafíos de seguridad que representan. La Computación en la Nube, permite externalizar los requisitos de computación y almacenamiento a los proveedores públicos y pagar por los servicios utilizados. El Internet de las cosas por sus siglas en inglés (IoT) Internet of Things, es un paradigma donde los objetos cotidianos pueden estar equipados con múltiples capacidades, permitiéndoles interconectarse con otros dispositivos mediante Internet para cumplir un propósito. El Bitcoin o la famosa Criptomoneda, revolucionó el campo de las monedas digitales, además de atraer una economía de mil millones de dólares. Otro hito de la evolución es la Seguridad Cognitiva, basaba en inteligencia en seguridad y Big Data, la Seguridad Cognitiva se caracteriza por su tecnología capaz de comprender, razonar y aprender. Todas estas tendencias tecnológicas presentan nuevos desafíos desde la perspectiva de la seguridad informática para el manejo, corrección y aseguramiento de los datos confidenciales de los usuarios. Este documento tiene como objetivo determinar los problemas asociados a estas tecnologías, las ventajas y desventajas, además se discute sobre los desafíos que presenta en el tema de seguridad informática.

**Palabras claves**: tecnología; iot; cloud computing; bitcoin; seguridad cognitiva; tendencias.

## Abstract

In the last decade technologies such as Internet of Things, Cloud Computing, Bitcoin have gained popularity due to the security challenges they represent. Computing in the Cloud, allows outsourcing the requirements of computing and storage to public providers and pay for the services used. The Internet of Things by its acronym in English (IoT) Internet of Things, Is a paradigm where everyday objects can be equipped with multiple capabilities, allowing them to interconnect with other devices through the Internet to fulfill a purpose. The Bitcoin or the famous Cryptocurrency revolutionized the field of digital currencies, in addition to attracting an economy of one billion dollars. Another milestone of evolution is Cognitive Safety, based on security intelligence and Big Data, Cognitive Security is characterized by its technology capable of understanding, reasoning and learning. All these technological trends present new challenges from the perspective of computer security for the management, correction and assurance of the

confidential data of users. The purpose of this document is to determine the problems associated with these technologies, the advantages and disadvantages, and also discusses the challenges presented in the topic of computer security.

**Keywords**: technology; iot; cloud computing; bitcoin; cognitive security; trends.

## Resumo

Na última década, tecnologias como a Internet das Coisas, Cloud Computing, Bitcoin ganharam popularidade devido aos desafios de segurança que representam. Computing in the Cloud, permite terceirizar os requisitos de computação e armazenamento para provedores públicos e pagar pelos serviços utilizados. A Internet das Coisas, por sua sigla em inglês (IoT) Internet of Things, é um paradigma onde os objetos do dia a dia podem ser equipados com múltiplas capacidades, permitindo que eles se interconectem com outros dispositivos através da Internet para cumprir um propósito. O Bitcoin ou o famoso Cryptocurrency, revolucionou o campo das moedas digitais, além de atrair uma economia de um bilhão de dólares. Outro marco da evolução é a Segurança Cognitiva, baseada em inteligência de segurança e Big Data, a Segurança Cognitiva é caracterizada por sua tecnologia capaz de entender, raciocinar e aprender. Todas essas tendências tecnológicas apresentam novos desafios sob a perspectiva da segurança computacional para a gestão, correção e garantia dos dados confidenciais dos usuários. O objetivo deste documento é determinar os problemas associados a essas tecnologias, as vantagens e desvantagens e também discute os desafios apresentados no tópico de segurança de computadores.

**Palavras chave**: tecnologia; iot; computação em nuvem; bitcoin; segurança cognitiva; tendências.

## Introducción

Las tecnologías emergentes en la última década han proporcionado una serie de ventajas para los usuarios, ya sea por su uso directo o porque permiten desarrollar aplicaciones. Entre las más reconocidas tenemos: G5, ERP (Enterprise Resource Planning), Industria Inteligente/Digital 4.0 o los famosos sistemas SCADA (Supervisory Control and Data Adquisition), Computación en la Nube (Cloud Computing), Fog Computing, Bitcoin, Big Data, Seguridad Cognitiva, IoT, etc. Sin

embargo, basados en la literatura existente, en el presente artículo se realiza un estudio comparativo entre las tecnologías: Internet de las cosas, Computación en la nube y Bitcoin.

Las apariciones vertiginosas de todas estas tecnologías, han desatado una serie de problemas y retos para el manejo adecuado y responsable. Errores de seguridad, perdida de datos, disminución de aspectos como privacidad, la inexistencia de estándares para su normalización y Responsabilidad Legal.

Internet of Things (IoT) o Internet de las Cosas, es una tecnología que emerge como un nuevo paradigma de la computación. Varios dispositivos y objetos son interconectados a través de Internet, la idea fundamental es mejorar la vida de las personas dotando de servicios tales como poder ir al supermercado y consultar el contenido de nuestra nevera usando el Smartphone. Controlar desde la TV hasta la luz del interior de la casa, usando una Echo Dot de fácil adquisición a través de Amazon.

Otro servicio que está en auge para el manejo y administración de datos es el uso de infraestructuras ubicadas en la nube. La computación en la nube, proporciona una solución flexible y rentable para muchos servicios a través de Internet. Es considerada como un cambio importante en la tecnología de la información (IT) y como el último modelo de computación sobre recursos computacionales agrupados, ancho de banda, almacenamiento, servicios y aplicaciones.

En esta misma década, internet ha sido testigo de la aparición de aplicaciones para la solución de problemas de manera cooperativa y distribuida. Las soluciones prácticas aplicables a menudo, han estado disponibles poco después de que la idea de una determinada aplicación, se haya concebido por primera vez. El dinero digital fue la excepción, desde la década de los 80, se tenía la idea haciendo realidad hace poco con la invención de la Criptomoneda. Consigo trae una serie de ventajas y desventajas que son necesarios conocer por todas las personas.

IBM por su parte a través de su proyecto Watson, introduce la Seguridad Cognitiva como un proceso que replica el funcionamiento del cerebro; usa la información no estructurada a través de técnicas de Machine Learning y Big Bata, procesa y devuelve resultados útiles estructurada. Esta tecnología es implementada en el resguardo de sistemas informáticos debido a la capacidad de autoaprendizaje en lo que se refiere a la seguridad de la información.

Todas estas aplicaciones y novedades tecnológicas han sido concebidas a la rapidez de la época moderna, sin embargo, no se ha podido medir su impacto y cuáles son los retos que trae consigo, por tanto, en el presente documento aborda apartados de gran interés para la comunidad científica tales como: puntos sensibles sobre estas tecnologías, ventajas, desventajas, los desafíos que representas estos avances, seguridad, privacidad y responsabilidad legal.

## Background

Esta sección provee de una introducción sobre conceptos importantes, necesarios para abordar el artículo científico.

### IoT Internet de las Cosas

El núcleo de la idea de Internet de las Cosas está basado en que las "cosas" cotidianas, como los vehículos, refrigeradoras, equipos médicos, y bienes de consumo estén equipadas con capacidades de seguimiento y detección. Las "cosas" también están cargadas con estas funciones de procesamiento y redes más sofisticadas, estos objetos inteligentes comprenden su entorno e interactúan con las personas. A igual que cualquier sistema de información IoT depende de una combinación de hardware, software y arquitecturas.

Gran parte del hardware sobre el que está construido IoT ya existe y se utiliza ampliamente. La infraestructura hardware critica incluye: RFID (del inglés Radio Frequency Identification), NFC (Near Field Communication) y redes de sensores.

El problema de IoT radica en el Software, si bien es cierto, el hardware no es nada novedoso comparado con el software que se debe desarrollar conjuntamente con el equipo, para que permita la interoperabilidad entre numerosos dispositivos heterogéneos y buscar los datos generados por ellos. Los principales softwares usados son Middleware, Searching/Browsing.

En cuanto a la Arquitectura de Hardware IoT usa Hardware/red, la más usada peer-to-per, EPCglobal y automática. En la parte de Software IoT usa Arquitectura Basada en Servicios SOA y el Modelo de Transferencia de Estado Representativo REST, estas son gratuitas presenta un enfoque en servicios y flexibilidad.

**Computación en la Nube**

Computación en la Nube o Cloud Computing, provee flexibilidad y efectivas soluciones a bajos costos a través de Internet. Este modelo presenta recursos computacionales agrupados, como ancho de banda, almacenamiento, servidores, potencia de procesamiento, servicios y aplicaciones. Esta tecnología ha eliminado la sobrecarga de planificación del usuario, proporcionando recursos disponibles bajo demanda, autoservicio y la capacidad de escalar según requerimientos del cliente. El modelo de negocios Pay-as-you-go justamente se refiere a pagar por lo que usas, esto ha permitido que las empresas pequeñas dispongan de grandes servicios a bajos costos y crecer bajo esta misma modalidad.

Los modelos de despliegue usados por computación en la nube son: Private Cloud centro de datos internos de una organización que no están disponibles para el público, Public Cloud disponible para uso público y Hibrid Cloud gestionada por la organización, haciendo público algunos accesos y otros de uso privado.

Los servicios de la computación en la nube, están organizados como: Infraestructuras como Servicio (IaaS), Plataformas como Servicio (PaaS), Software como Servicio (SaaS) y los nuevos servicios conocidos como; Integridad de Datos como Servicio (DIaaS), Base de Datos como Servicio, Logging como Servicio y Procedencia como Servicio, Seguridad como Servicio y Big Data como Servicio.

En el almacenamiento en la nube los datos pueden estar dispersos en ubicaciones y servidores remotos. El usuario pierde el control de los datos y no puede inspeccionar visualmente los enlaces de datos.

Varios modelos de almacenamiento de datos son usados por servicios de almacenamiento en la nube, esto también incluye sistemas de archivos, bases de datos relacionales y base de datos de gráficos.

**Bitcoin**

En noviembre del 2008, Satoshi Nakamoto anuncio la creación de una Criptomoneda. Para el 2009 el Bitcoin se convirtió rápidamente en viral. Nakamoto permaneció activo hasta el 2010

antes de entregar el proyecto. Hasta ahora, la identidad de Nakamoto permanece desconocida, lo que se tiene claro es que Bitcoin es el resultado de la contribución de años de investigación.

Se resolvió los problemas fundamentales de una manera altamente sofisticada, original y prácticamente viable: utiliza un esquema de prueba de trabajo para limitar el número de votos por entidad, y así hace que la descentralización sea práctica. Los mineros de Bitcoin recolectan transacciones en un bloque y varían una pausa hasta que uno de ellos encuentre la solución a un rompecabezas dado. El bloque que incluye la solución y las transacciones se transmiten a todas las demás entidades, y el libro mayor distribuido (la cadena de bloques) se actualiza. La propiedad de las monedas se puede determinar atravesando la cadena de bloques hasta que se encuentre la transacción más reciente de la moneda respectiva. Las horquillas de la cadena de bloques debido a manipulaciones maliciosas o retrasos en la propagación se resuelven considerando la bifurcación "más larga" (incluida la mayor parte del trabajo) como consenso. Por lo tanto, Sybil y, al menos hasta cierto punto, los ataques de doble gasto se mitigan mediante adiciones vinculantes a la cadena de bloques (votos) a las contribuciones a la prueba de trabajo. La prueba de trabajo también induce un suministro continuo de nuevas monedas como recompensa (e incentivo) para los mineros. Todo esto no requiere una autoridad de coordinación centralizada, y prácticamente demuestra la viabilidad de una moneda digital distribuida.

El protocolo de Bitcoin básicamente fue introducido por el mismo Nakamoto, su idea principal: el uso de la prueba de trabajo para eliminar el banco y descentralizar y asegurar el libro mayor. En particular, introduce sucesivamente los conceptos básicos sobre minería, cadena de bloques, transacciones y scripting. La documentación del desarrollador de Bitcoin, el Bitcoin wiki y el código fuente de Bitcoin (github.com/bitcoin/ bitcoin).

El punto de partida es monedas digitales centralizadas, como ejemplo vamos a suponer que Alice quiere transmitir una moneda a Bob. A fin de hacerlo y usando una manera ingeniosa, podría generar un contrato firmado digitalmente que establezca la transacción que va hacer. Lo anunciara públicamente, siguiendo la terminología del Bitcoin, dicho contrato se puede llamar (TX) Transacción X. Se puede considerar como un contrato firmado que es verificable usando la clave pública de Alice, sin embargo, no es a prueba de falsificación. Esto podría lograrse introduciendo números de serie, pero ¿de dónde provienen? Necesitamos una fuente confiable

que emita las publicaciones seriadas. En un escenario centralizado, esto es lo que genéricamente se llama banco: el banco emite monedas con números de serie únicos, y mantiene un libro contable que incluye todas las propiedades, i. e., el mapeo entre cuentas de usuario y números de serie.

**Seguridad Cognitiva**

Termino adoptado por IBM (International Business Machines), para describir sistemas de autoaprendizaje que utilizan minería de datos, aprendizaje de máquina, procesamiento del lenguaje natural e interacción ser humano-ordenador para imitar el funcionamiento del cerebro humano.

La cognición se refiere a todos los procesos sensoriales que se transforman, reducen, elaboran, clasifican, almacenan, recuperan y se utiliza desde el punto de vista de la información.

Estas tecnologías cognitivas, se desarrollan sobre la base de los sistemas de información inteligentes. El propósito no es solo el análisis de datos, procesamiento y registro, sino principalmente un análisis mediante la comprensión y el razonamiento, sobre el contenido semántico de los datos procesados.

Cada sistema de información que analiza cierta información, posee en su base de datos del conocimiento, ciertos parámetros o conocimiento, indispensable para ejecutar un correcto análisis y tener resultados concisos.

La seguridad cognitiva puede ser implementada de dos formas: i) Como Sistemas Cognitivos que sirven para analizar información, convergen grandes volúmenes de datos son procesados. Los resultados son tendencias de seguridad, negocio, respuestas a problemas en basa a esta información entre otros. ii) Aplicación de tecnologías cognitivas en sistemas, los cuales actúen de forma independiente dando seguridad activa y proactiva al entorno en el cual actúen.

## Tendencias, Ventajas Y Desventajas De IoT, Cloud Computing Y Bitcoin

En esta sección se discute; las tendencias de las tecnologías mencionadas y cuáles son los desafíos que presentan para los profesionales de la seguridad informática.

Como se puede apreciar en la Fig. 1. tanto IoT, Computación en la Nube y Bitcoin son tendencias actuales que se han desarrollado a gran escala, trayendo beneficios a sus usuarios o clientes, sin embargo, solo se ha pensado en la función que realiza y no ha existido el tiempo para hacer pruebas y tener una visión general de todos los aspectos relacionados, a las aplicaciones tecnológicas. Esto ha desatado el interés por la comunidad científica interesándose por estudiar.

**i) IoT**

Crea nuevos desafíos legales que se deben abordar. En particular, la gobernanza de un recurso como es esta tecnología no debe estar dictada por un grupo, sino más bien, con estándares que permitan dar soporte de calidad. La responsabilidad global y el cumplimiento son aspectos fundamentales que complementado a lo anterior permite mejorar la efectividad de la gobernanza a través de las amenazas y sanciones.

a) **Ventajas:** IoT presenta como principal ventaja, interconectar muchos dispositivos a internet y tener información de primera mano. Esta ventaja ha sido utilizada en el área de la salud. La industria también está haciendo uso de este principio para la mejora del proceso de manufacturación. Los costos de los productos IoT son relativamente bajos, esto hace que esté al alcance de la mayoría de las personas.

b) **Desventajas:** El consumo de energía es un problema que presentan los dispositivos IoT. Por ser una tecnología que aún está en desarrollo, al momento posee recursos limitados en lo que se refiere batería, memoria y capacidad de procesamiento. Los problemas de administración también están presentes en IoT, como todos los dispositivos están conectados a internet, no tenemos un completo control de los mismos.

c) **Vulnerabilidades**: las principales vulnerabilidades de estas tecnologías se encuentran en los protocolos de conectividad que usan. La encriptación de los datos no es al 100% en muchos dispositivos, es decir, se transmiten datos en claros.

d) **Ataques**: los ataques más comunes a estos dispositivos es Denegación de Servicios (DOS), por su tecnología hace que estos dispositivos sean conductores de datos maliciosos que envenenan la red y dejan híbridos a todos los dispositivos. Otro ataque conocido es Extensión de Funcionalidad, utiliza la funcionalidad del dispositivo para

lograr un efecto totalmente diferente. Un caso encontrado en la literatura en el uso de luces inteligentes de un hogar, puede tomar el control el atacante, encender las luces a una frecuencia para desencadenar convulsiones en personas que sufren de epilepsia fotosensible (de la misma manera que los videojuegos que parpadean rápidamente pueden causar tales ataques). Complementando a estos ataques tenemos Ataque RIPL o RPL (Remote Internal Program Load).

**ii) Computación En La Nube**

a) **Ventajas**: la principal ventaja es en los costos que representa para una empresa, en cuanto a no gastar en infraestructura y solo pagar por el servicio que usa. Teletrabajo es una característica que presenta esta tecnología, permite la administración de datos, recursos o información desde cualquier parte del mundo a los usuarios propietarios.

b) **Desventajas**: en cuanto a los desafíos que presenta la Computación en la nube es que los datos están dispersos en distintas ubicaciones, esto hace que el cliente no tenga un control sobre los mismos. Además, los proveedores de este servicio, por ahorrar costos operacionales migran sus servidores a países que contemplan otras leyes en cuanto a comercio electrónico. Esto ocasiona el deterioro de una propiedad importante en cuento a la información que es la privacidad de los datos y más si se trata de números de tarjetas de crédito, etc. Otro desafío importante que presenta el almacenamiento en la nube, es el desconocimiento de la infraestructura que hay detrás del proveedor del servicio. No sabemos que procedimientos tiene para deshacerse de equipos viejos o su reutilización esto puede ocasionar la perdida de información o ser blanco fácil por las vulnerabilidades que presenta para ser hackeadas. No existen estándares que permitan depurar estos problemas, desde el almacenamiento de la información hasta como mantenerla en la nube, se hace bajo esquemas propios de cada proveedor. Esto trae un problema adicional, el hecho de no poder migrar de proveedor ya que los procesos no son generales causando dependencia al que ofrece el servicio.

c) **Vulnerabilidades**: La infraestructura sigue siento física en algún lugar del mundo, a pesar de que se usa entornos de virtualización, los servidores son físicos, por tanto, las vulnerabilidades están presentes como en el resto de servidores, en la nube que hacen

difícil o imposible implementar controles de seguridad (probados y comprobados); por ejemplo, los procedimientos de gestión que se crearon inicialmente para una estructura de hardware fija no se transfieren correctamente a las máquinas virtuales.

d) **Ataques**: los ataques más frecuentes en la nube son los de DOS, en estos entornos las máquinas virtuales (VM) también representan un peligro ya que los atacantes pueden usar el ataque denominado Salto VM y conseguir fuga de datos.

**iii) Bitcoin**

a) **Ventajas**: el Bitcoin reemplaza la moneda fiduciaria en múltiples dimensiones; porque se puede transferir internacionalmente sin ningún límite, las transacciones no tienen tarifas o una tarifa muy baja, actualmente no necesita ninguna información personal (útil para el anonimato), es transparente ya que cada usuario tiene una copia del libro mayor público y seguro como el algoritmo criptográfico subyacente. Bitcoin es el primer sistema de moneda completamente descentralizado y fuera del control de cualquier poder monetario. Aprendiendo del fracaso del sistema económico centralizado

b) **Desventajas**: Bitcoin lo que se ha garantizado al momento es el Anonimato, sin embargo, ha desatado una serie de conflictos: Riesgos de seguridad y las implicaciones de seguridad del protocolo de Bitcoin y del diseño del sistema. Bitcoin es una moneda digital, con un valor notable en el mercado, todo esto son motivos suficientes para intentar explotar las vulnerabilidades presentes en esta invención, al momento se ha comprobado que de los ataques el 51% es a esta Criptomoneda. El Bitcoin no asegura la privacidad, es cierto que oculta identidades, pero no es privado.

El Bitcoin se ha convertido en una moneda inestable por lo que tiende a subir o a bajar en el mercado, esto da lugar a especulaciones. Aquí no existe la minería económica como lo hay en las monedas de los diferentes países. Sin la minería, las identidades falsas pueden subvertir el consenso y destruir el sistema.

c) **Vulnerabilidades**: Las vulnerabilidades presentes en esta Criptomoneda, la mayoría son teóricas, sin embargo, hay muchas que se han llevado a cabo. El ataque denominado 51% es la vulnerabilidad más conocida.

d) **Ataques**: como se mencionó anteriormente el ataque más conocido es el de 51% que en algunos casos ha sido ejecutado con éxito. Suplantación de identidad es un ataque latente en esta tecnología. Ataques al cifrado de esta Criptomoneda se ha registrado, por lo que denota, muchos ataques y que va en aumento.

**iv) Seguridad Cognitiva**

a) **Ventajas**: una de las ventajas importantes en seguridad cognitiva es que ayuda solidificar la seguridad y el aprovechamiento efectivo de los miles de datos (big data) ya que no basta con aprender, corregir y vigilar sino también supervisar las amenazas para prevenir futuros ataques, proporciona una disciplina de aprendizaje automático (machine learning) puesto que cada día pedimos que los dispositivos informáticos aprendan por sí solas y se acerquen a la forma de pensamiento y comunicación humana.

b) **Desventajas**: como desventajas se puede mencionar el limitado número de expertos en esta rama, el desarrollo automatizado, es decir, que una vez realizado el modelo de seguridad se necesita implementar, lo cual se necesita de otro experto que debe entender y así que no tome mucho tiempo la: renovación de los modelos, escalabilidad y por último y más importante que la máquina llegue a suplantar al hombre y así puedan acabar con algunos puestos de trabajo.

c) **Vulnerabilidades**: las vulnerabilidades en seguridad cognitiva, por lo general no son identificadas con frecuencia, ya que los analistas de seguridad utilizan métodos para el aprendizaje, agrupación de clúster, minería de gráficos y modelados relaciones de entidades para identificar las vulnerabilidades potenciales.

d) **Ataques:** los sistemas cognitivos pueden analizar grandes cantidades de datos maliciosos malware y detectarlos a tiempo. Es por eso que no se detectan aun ataque a sistemas que utilizan seguridad cognitiva. De la misma forma que crece la seguridad cognitiva los atacantes también están utilizando las mismas técnicas de sistemas cognitivos y proveyéndose de aprendizajes e inteligencia para personificar y mejorar sus ataques, están siendo reforzados con inteligencia artificial, redes neuronales.

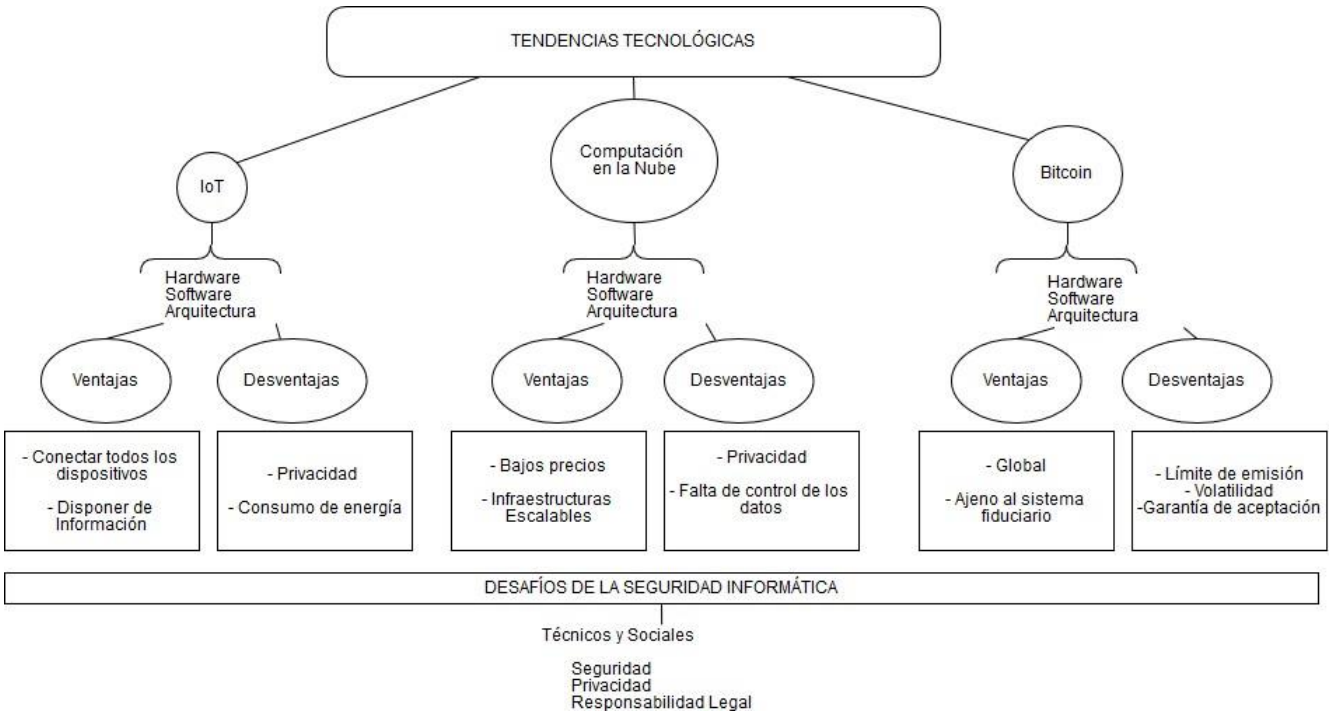


**Fig. 1** Tendencias Tecnológicas IoT, Computación en la Nube y Bitcoin.

## Desafíos De IoT, Cloud Computing Y Bitcoin

Los desafíos que representan estas tecnologías se han resumido a Seguridad, Privacidad y Responsabilidad Legal.

### i) Seguridad

La seguridad en cualquier tecnología debe estar presente, no solo por la información que contiene o procesa, sino también porque en la actualidad está directamente relacionada con la privacidad del usuario.

IoT es un área delicada a la cual se debe prestar total interés, esta tecnología ha incursionado en la Medicina e Industria que son puntos débiles de un país, los cuales no deben ser manipulados ni cambiados por personas ajenas a los mismos. Este principio también rige para la Computación en la Nube, los datos de empresas, instituciones u organizaciones, están almacenados en estos entornos. Bitcoin al parecer es más fuerte en este aspecto, sin embargo, se ha demostrado que tiene problemas de seguridad que necesitan ser analizados y solucionados.

**ii) Privacidad**

Todas estas tecnologías exponen datos delicados de sus usuarios. En la bibliografía revisada, se hace hincapié que la Privacidad es un principio de la seguridad informática que se debe garantizar. IoT no tiene estándares que garanticen esto, al igual que almacenamiento en la Nube y que decir sobre Bitcoin que no está normado bajo ninguna ley o reglamento existente en el mundo.

**iii) Responsabilidad Legal y Gobernanza**

Ninguna de estas 3 tecnologías tiene estándares definidos para su desarrollo, implementación y uso. Por tanto, no están normados, esto hace que sea nula la existencia de leyes que las rijan y se pueda hacer uso de ellas en el caso de incumplimiento de cualquiera de ellas. Mientras no exista responsabilidad legal para advertir o sancionar a infractores de estas tecnologías ya sea: fabricante, proveedor o cliente, no se podrá garantizar seguridad ni privacidad.

## Conclusiones

El avance tecnológico que se da en cualquier década, trae consigo desafíos que no se han contemplado al momento del desarrollo sino, cuando ya está en producción. Esto representa verdaderos retos para los diferentes componentes que lo integran.

El software y hardware de Bitcoins no está desarrollado de una manera eficaz, esto deja muchas brechas de seguridad y problemas al usarlos.

IoT, Computación en la Nube y Bitcoin no tiene reglamentos, estándares, leyes propias, el marco para manejo de datos consiste en regulaciones generales adoptadas en el campo de procesamiento de datos personales.

Para el futuro, no sabemos si estas tecnologías van a persistir o tomar fuerza, pero al momento, debemos asegurar para cumplir con los objetivos de la seguridad informática que es: Confidencialidad, Integridad y Disponibilidad.

El campo para hacer investigación científica en lo que se refiere a estas tecnologías está abierto, habiendo muchos temas de trascendental importancia por abordar.

## Referencias Bibliográficas

F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

Y. M. Kow and C. Lustig, “Imaginaries and Crystallization Processes in Bitcoin Infrastructuring,” Comput. Support. Coop. Work, pp. 1–24, Oct. 2017.

F. J. FaheemZafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Masoom Alam, “A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends,” Comput. Secur., vol. 65, pp. 29–49, Mar. 2017.

I. Yaqoob et al., “Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges,” IEEE Wirel. Commun., vol. 24, no. 3, pp. 10–16, 2017.

A. A. Faheem Zafar, Abid Khan, Saba Suhail, Idrees Ahmed, Khizar Hameed, Hayat Mohammad Khan, Farhana Jabeen, “Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes,” J. Netw. Comput. Appl., vol. 94, pp. 50–68, Sep. 2017.

S. Sengupta, V. Kaulgud, and V. S. Sharma, “Cloud Computing Security--Trends and Research Directions,” in 2011 IEEE World Congress on Services, 2011, pp. 524–531.

A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things—A survey of topics and trends,” Inf. Syst. Front., vol. 17, no. 2, pp. 261–274, Apr. 2015.

L. Van Der Horst, K.-K. R. Choo, and N.-A. Le-Khac, “Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core,” IEEE Access, vol. 5, pp. 22385–22398, 2017.

P. K. Kaushal, A. Bagga, and R. Sobti, “Evolution of bitcoin and security risk in bitcoin wallets,” in 2017 International Conference on Computer, Communications and Electronics (Comptelix), 2017, pp. 172–177.

A. Viswam and G. Darsan, “An efficient bitcoin fraud detection in social media networks,” in 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2017, pp. 1–4.

Z. H. Ali, H. A. Ali, and M. M. Badawy, “A New Proposed the Internet of Things (IoT) Virtualization Framework Based on Sensor-as-a-Service Concept,” Wirel. Pers. Commun., vol. 97, no. 1, pp. 1419–1443, Nov. 2017.

S. Iraji, P. Mogensen, and R. Ratasuk, “Recent Advances in M2M Communications and Internet of Things (IoT),” Int. J. Wirel. Inf. Networks, vol. 24, no. 3, pp. 240–242, Sep. 2017.

Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, “A method for trust management in cloud computing: Data coloring by cloud watermarking,” Int. J. Autom. Comput., vol. 8, no. 3, pp. 280–285, Aug. 2011.

N. Shi, “A new proof-of-work mechanism for bitcoin,” Financ. Innov., vol. 2, no. 1, p. 31, Dec. 2016.

S. Shokrollahi and F. Shams, “Rich Device-Services (RDS): A Service-Oriented Approach to the Internet of Things (IoT),” Wirel. Pers. Commun., vol. 97, no. 2, pp. 3183–3201, Nov. 2017.

T. Yang, H. Pen, W. Li, D. Yuan, and A. Y. Zomaya, “An Energy-Efficient Storage Strategy for Cloud Datacenters Based on Variable K-Coverage of a Hypergraph,” IEEE Trans. Parallel Distrib. Syst., vol. 28, no. 12, pp. 3344–3355, Dec. 2017.

X. Zhou, Q. Wu, B. Qin, X. Huang, and J. Liu, “Distributed Bitcoin Account Management,” in 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 105–112.

Y. Zhu, D. Dickinson, and J. Li, “Analysis on the influence factors of Bitcoin’s price based on VEC model,” Financ. Innov., vol. 3, no. 1, p. 3, Dec. 2017.

J. G. Fraser and A. Bouridane, “Have the security flaws surrounding BITCOIN effected the currency’s value?,” in 2017 Seventh International Conference on Emerging Security Technologies (EST), 2017, pp. 50–55.

S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of Things (IoT) communication protocols: Review,” in 2017 8th International Conference on Information Technology (ICIT), 2017, pp. 685–690.

H. N. Saha et al., “Pollution control using Internet of Things (IoT),” in 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017, pp. 65–68.

H. N. Saha et al., “Waste management using Internet of Things (IoT),” in 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017, pp. 359–363.

W. Abderrahim and Z. Choukair, “The three-dimensional model for dependability integration in cloud computing,” Ann. Telecommun., vol. 72, no. 5–6, pp. 371–384, Jun. 2017.

S. Kethineni, Y. Cao, and C. Dodge, “Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes,” Am. J. Crim. Justice, pp. 1–17, May 2017.

I. Sohn, S. W. Yoon, and S. H. Lee, “Distributed scheduling using belief propagation for internet-of-things (IoT) networks,” Peer-to-Peer Netw. Appl., pp. 1–10, Oct. 2016.

G. Yao, Y. Ding, and K. Hao, “Using Imbalance Characteristic for Fault-Tolerant Workflow Scheduling in Cloud Systems,” IEEE Trans. Parallel Distrib. Syst., vol. 28, no. 12, pp. 3671–3683, Dec. 2017.

Y. Zhang and J. Wen, “The IoT electric business model: Using blockchain technology for the internet of things,” Peer-to-Peer Netw. Appl., vol. 10, no. 4, pp. 983–994, Jul. 2017.

W. Kinsner, “Towards cognitive security systems,” in 2012 IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing, 2012, pp. 539–539.

J. M. Chang et al., “Capturing cognitive fingerprints from keystroke dynamics,” IT Prof., vol. 15, no. 4, pp. 24–28, 2013.

D. Krawczyk, J. Bartlett, M. Kantarcioglu, K. Hamlen, and B. Thuraisingham, “Measuring expertise and bias in cyber security using cognitive and neuroscience approaches,” in 2013 IEEE International Conference on Intelligence and Security Informatics, 2013, pp. 364–367.

L. Ogiela and M. R. Ogiela, Advances in cognitive information systems, vol. 17. Springer Science & Business Media, 2012.

IBM, “Cognitive_Security,” in IBM security, Estados Unidos, 2016, p. 11.

L. Ogiela and M. R. Ogiela, “Cognitive Systems and Artificial Brains,” Springer, Berlin, Heidelberg, 2012, pp. 99–106.

M. Radovan and B. Golub, “Trends in IoT security,” in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017, pp. 1302–1308.

W. Hlaing, S. Thepphaeng, V. Nontaboot, N. Tangsunantham, T. Sangsuwan, and C. Pira, “Implementation of WiFi-based single phase smart meter for Internet of Things (IoT),” in 2017 International Electrical Engineering Congress (iEECON), 2017, pp. 1–4.

L. Ogiela and M. R. Ogiela, “Cognitive Information Systems,” Springer, Berlin, Heidelberg, 2012, pp. 51–60.

L. Ogiela and M. R. Ogiela, “Intelligent Cognitive Data Analysis Systems of the UBMSS Type as an Example of Cognitive Categorisation Systems,” Springer, Berlin, Heidelberg, 2012, pp. 61–73.

T. Yamauchi, “The Semantic Web and Human Inference: A Lesson from Cognitive Science,” Springer, Berlin, Heidelberg, 2007, pp. 609–622.

H. Zhang, A. Hussain, D. Liu, and Z. Wang, Eds., Advances in Brain Inspired Cognitive Systems, vol. 7366. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

C. Stary, “Special issue on recent advances in cognitive engineering,” J. Interact. Sci., vol. 3, no. 1, p. 4, Dec. 2015.

L. Ogiela and M. R. Ogiela, “Towards cognitive service management and semantic information sharing in the Cloud,” Multimed. Tools Appl., pp. 1–11, Oct. 2017.

Y. Wu and I. Niemegeers, “A Cognitive Architecture for Personal Networks,” Springer, Berlin, Heidelberg, 2006, pp. 12–24.

A.-M. Horcher and G. P. Tejay, “Building a better password: The role of cognitive load in information security training,” in 2009 IEEE International Conference on Intelligence and Security Informatics, 2009, pp. 113–118.

T. E. Carroll, F. L. Greitzer, and A. D. Roberts, “Security informatics research challenges for mitigating cyber friendly fire,” Secur. Inform., vol. 3, no. 1, p. 13, Dec. 2014.

G. Cybenko, A. Giani, and P. Thompson, “Cognitive hacking,” Adv. Comput., vol. 60, pp. 35–73, 2004.

A. D. W. Sumari and A. S. Ahmad, “Cogitive Artificial Intelligence: The fusion of Artificial Intelligence and information fusion,” in Electronics and Smart Devices (ISESD), International Symposium on, 2016, pp. 1–6.

L. Ogiela and M. R. Ogiela, “Towards cognitive cryptography,” J. Internet Serv. Inf. Secur., vol. 4, no. 1, pp. 58–63, 2014.

K. G. Kroeck, P. J. Kirs, and A. M. Fiedler, “Cognitive biasing effects in information systems: implications for linking real world information with human judgment,” in System Sciences, 1989. Vol. III: Decision Support and Knowledge Based Systems Track, Proceedings of the Twenty-Second Annual Hawaii International Conference on, 1989, vol. 3, pp. 517–524.

A. M. Gamundani, “An impact review on internet of things attacks,” in 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 2015, pp. 114–118.

A. Ukil, J. Sen, and S. Koilakonda, “Embedded security for Internet of Things,” in 2011 2nd National Conference on Emerging Trends and Applications in Computer Science, 2011, pp. 1–6.

S. Alanazi et al., “On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications,” in 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 205–210.

E. Ronen and A. Shamir, “Extended Functionality Attacks on IoT Devices: The Case of Smart Lights,” in 2016 IEEE European Symposium on Security and Privacy (EuroS&P), 2016, pp. 3–12.

I. E. Baciu, “Advantages and Disadvantages of Cloud Computing Services, from the Employee’s Point of View.” 2015.

K. Dahbur, B. Mohammad, and A. B. Tarakji, “A survey of risks, threats and vulnerabilities in cloud computing,” in Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA ’11, 2011, pp. 1–6.

M. Bedford Taylor, “The Evolution of Bitcoin Hardware,” Computer (Long. Beach. Calif). vol. 50, no. 9, pp. 58–66, 2017.

D. Bradbury, “The problem with Bitcoin,” Comput. Fraud Secur., vol. 2013, no. 11, pp. 5–8, Nov. 2013.

.