14

Fecha de presentación: enero, 2017
Fecha de aceptación: febrero, 2017
Fecha de publicación: abril, 2017

IMPLEMENTACIÓN

DEL PROYECTO DE RED INVISIBLE PARA EL ASEGURAMIENTO DE PRIVACIDAD Y CALIDAD EN LAS COMUNICACIONES SOBRE INTERNET

IMPLEMENTATION OF INVISIBLE NETWORK PROJECT FOR PRIVACY AND QUALITY ASSURANCE IN INTERNET COMMUNICATIONS

MSc. Marlon Altamirano Di Luca[1]
E-mail: marlon.altamiranod@ug.edu.ec
MSc. Shirley Huerta Cruz[2]
E-mail: shirley.huerta@ute.edu.ec
[1] Universidad de Guayaquil. República del Ecuador.
[2] Universidad Tecnológica Equinoccial. República del Ecuador.

Cita sugerida (APA, sexta edición)

Altamirano Di Luca, M., & Huerta Cruz, S. (2017). Implementación del Proyecto de Red Invisible para el aseguramiento de privacidad y calidad en las comunicaciones sobre internet. Universidad y Sociedad, 9(2), 110-114. Recuperado de http://rus.ucf.edu.cu/index.php/rus

RESUMEN

En el artículo se hace referencia al análisis de factibilidad para la implementación de la tecnología del Proyecto de red invisible (I2P) en la carrera de Networking y Telecomunicación. Se presentan características generales del anonimato de la herramienta TOR y los estándares con los que funciona de tal forma que el intercambio de información entre usuarios sea confiable y que la integridad de los datos transferidos no sea vulnerada. La propuesta detalla además las etapas de implementación donde se consideran aspectos técnicos, legales, sociales y a su vez el costo de la implementación. Así mismo se detalla las fases de implementación de la tecnología I2P necesarias dentro de la carrera de networking y telecomunicación.

Palabras clave: I2P, privacidad comunicaciones, redes, internet.

ABSTRACT

The article refers to the feasibility analysis for the implementation of the Invisible Network (I2P) Project technology in Networking and Telecommunication. There are general characteristics of the anonymity of the TOR tool and the standards with which it works in such a way that the exchange of information between users is reliable and that the integrity of the data transferred is not violated. The proposal also details the stages of implementation where technical, legal, social aspects and, in turn, the cost of implementation are considered. It also details the phases of implementation of I2P technology required in the networking and telecommunication career.

Keywords: I2P, privacy communications, networks, internet.

INTRODUCCIÓN

La utilización de las Tecnologías de la Información y las Comunicaciones (TIC), no ha pasado desapercibida para los diferentes grupos organizados que encuentran en ellas las herramientas que mejoran sus procesos de funcionamiento interno en cualquier ente público o privado a nivel de usuarios.

Por esta razón, el estudio de su investigación se fundamenta en un interrogante principal: ¿La Comunicación es realmente confiable y segura?

Se realiza el estudio basado en la seguridad utilizando la tecnología I2P para garantizar confiabilidad al momento de compartir datos informáticos. Sin embargo, la preocupación de los nuevos programas de vigilancia en la web y los reglamentos que pueden ejercer los gobiernos sobre las plataformas tales como Facebook, Google; entre otros.

Por esto se ha reforzado el interés de algunos grupos por proteger su anonimato. Algunos de ellos ya han desplegado infraestructuras tecnológicas que les permiten proteger la integridad de sus datos.

Desde el aspecto social nos cuestionamos si una comunicación de calidad, es bien tratada o distribuida por los diferentes medios tecnológicos que trascienden y rompen paradigmas en este mundo globalizado.

El objetivo de esta investigación se presta a múltiples repuestas y a variadas soluciones que permite, realizar la comunicación, transferencia de datos con una seguridad confiable, permite que no haya terceros en la red al momento de realizar la actividad, es decir que el anonimato sea seguro entre usuarios y no haya suplantación de identidad.

El proyecto I2p se encuentra desarrollándose día a día para garantizar el 100% de seguridad e integridad de los datos.

Al momento de compartir o transferir información entre usuarios con un anonimato confiable y una comunicación de alta seguridad mediante esta tecnología, se tiene la satisfacción de que la información es vista y leída por el destinatario, sin que la información sea manipulada o peor aún, sepan quien lo envía es decir un anonimato seguro.

Es así que nace el deseo de averiguar hasta donde la tecnología puede llegar para resguardar nuestros datos informáticos, que son muy importantes para cada usuario y ente de cada organización.

En la actualidad, con la aparición del internet, los métodos de comunicación han ido actualizándose, haciéndose cada vez más, parte integral de nuestro estilo de vida. Al convertirse en un medio común para la compartición de información, es necesario analizar aspecto como la seguridad y la integridad de la información que se encuentra viajando por toda la red.

Existen diversos métodos que nos ofrecen un cierto nivel de anonimato, entre ellos está el Proyecto de internet Invisible (I2P),el cual consiste en una red anónima que se encarga de ocultar la identidad del remitente y el receptor, es un sistema totalmente distribuido, encarga de retransmitir el tráfico a través de múltiples nodos utilizando túneles (De Luz, 2012).

Para su correcto aseguramiento de las comunicaciones que se realizan a través de la red requieren que estas tengan un alto grado de seguridad, tanto como para los usuarios que se encuentran dentro de una institución, como para el usuario común que desea compartir información sin que esta sea vigilada o monitorizada por extraños.

Por lo cual se propone analizar el uso de la infraestructura de red I2P, para asegurar las comunicaciones en la red.

El resultado de no tener un control en tiempo real se ve reflejado en la inseguridad de los datos que navegan dentro de una red. Por lo cual el proyecto I2P (Proyecto de Internet Invisible, 2010) está pensado para proteger la información de forma anónima, y así evitar que terceras personas mal utilicen la información tanto para instituciones públicas como para privadas es el caso de la Universidad de Guayaquil facultad de Ciencias Matemáticas y Físicas.

Por esta razón apoyada en la implementación de la tecnología se propone el siguiente proyecto basado en I2P (Proyecto de Internet Invisible, 2010), para protección de los datos que navegan a través de la red ya que la información es enviada a través de uno de los túneles de salida hacia uno de los túneles de entrada del cliente, impide que sea capturado el paquete y su información.

El I2P (Siglas de Invisible Internet Project, en español Proyecto de Internet Invisible) es un software con capa de abstracción para realizar las comunicaciones entre ordenadores, es decir, punto a punto, para crear así la creación de herramientas y aplicaciones de red con un fuerte anonimato (Mejía Barrera & Peralta Palacios, 2014).

El objetivo primordial en esta tecnología I2P es una red anónima, para la aplicación de envió de mensajes entre sí de forma anónima y segura. Así como veíamos en el caso del navegador TOR dentro de su propia red TOR, I2P es una plataforma que presta múltiples usos para diferentes aplicaciones. I2P nos permite mensajería IP, pero también brinda soporte a datagramas TCP y su comunicación está cifrada extremo a extremo (Sánchez Cañestro, 2015).

DESARROLLO)

El Proyecto de Internet Invisible (I2P) es una nueva propuesta tecnológica el cual permite desarrollar un anonimato confiable entre usuarios concede seguridad al momento de transferir archivos dentro de la carrera de Networking y telecomunicaciones de forma eficiente, con respecto a su servicio por la cual existe la factibilidad técnica para el desarrollo de dicho proyecto metodológico, puesto que tiene una arquitectura disponible para poder implementar en la entidad educativa.

Hace muchos años varios investigadores intentaban encontrar la forma de compartir los datos informáticos de una forma eficiente y privada. Con la evolución del Internet se busca la forma de realizar una comunicación privada, es decir sin terceras personas espiando el contenido de sus datos (Proyecto de Internet Invisible, 2010).

Es entonces que navegar y comunicarse de forma anónima era cada vez más complicado, la tecnología que permitía realizarlo era la llamada darknet o Red Oscura, aunque el mercado ofrece herramientas que admite realizarlo (Proyecto de Internet Invisible, 2010).

Con la evolución del internet se ha descubierto grandes herramientas que permite compartir información y contenidos digitales con medidas para preservar el anonimato de quienes intercambian información como es el caso Tor, por ser una red distribuida de baja latencia donde el encaminamiento de mensajes por la red otorga la protección de identidad de los usuarios, consiente cifrar la información en los nodos de entrada y se descifran en los nodos de salida (Brezo Fernández & Rubio Viñuela, 2011).

También está el caso de Freenet al igual que Tor es una red de distribución de información de anonimato entre usuarios pero contiene una particularidad, al permitir poner a disposición de la red parte de su ancho de banda y su capacidad de almacenamiento, dando opción a configurar para que la misma funcione como una red F2F (***Amigo a Amigo***) (Brezo Fernández, et al., 2011).

El origen de estos sistemas en realidad consiste en proporcionar mayor seguridad a los usuarios sin embargo, al ser visible la privacidad con la uno puede trabajar y el hecho de no estar fuera de vista de los otros, ha favorecido que este tipo de negocio se encuentre en los lugares menos visibles del mundo real (Proyecto de Internet Invisible, 2010).

Esto ayuda a proteger los datos que transitan en la red de vigilancia y la monitorización por partes externas como los ISPs (quienes proveen el servicio de Internet). El anonimato se vuelve más fuerte al hacerse una red muy grande. El proyecto I2P ayuda a tener un nivel muy alto de privacidad en las comunicaciones del internet, para esto se considera una red resistente, bien organizada, con alto protección de anonimato. Hay actividades que pueden ponerse en riesgo por su privacidad al hacerse anónimamente dentro del proyecto I2P (proyecto de internet invisible).El funcionamiento de la red I2P es un proyecto para formar, direccionar y mantener una red que soporte comunicación segura y anónima (Mejía Barrera, et al., 2014).

Los clientes de I2P pueden distribuir el equilibrio entre el anonimato, uso de ancho de banda y latencia. El sistema no presenta un punto central por la cual pueda surgir alguna presión que se vaya a recibir afectación la integridad, seguridad y el anonimato de la tecnología, por esta razón la red es abierta y se encuentra en libre disposición (Proyecto de Internet Invisible, 2010).

Se debe tomar en cuenta que, a diferente de las otras redes anónimas, I2P no permite un anonimato invisible al cliente para su mensaje y no al destinatario, o vice versa. Esto quiere decir que I2P se encuentra estructurada para realizar a los pares de comunicarse unos con otros anónimamente ambos, es decir quien envía y quien recibe, ya que no son vistos entre ellos, ni por terceras personas (Proyecto de Internet Invisible, 2010).

La red es si se encuentra orientada a mensajes, es por esta razón que posee capa IP de segura y anónima lo cual los mensajes son direccionados a claves Criptográficas (Destino) ya que pueden ser más intensos los paquetes IP. Y con ayuda de aplicación I2PTunel, son capaces de hacer correr aplicaciones TCP/IP que es lo tradicional sobre la tecnología I2P, también tenemos SSH, IRC, un proxy Squid e igualmente Streaming de audio (Proyecto de Internet Invisible, 2010).

Su objetivo esencial en diseñar, desarrollar y utilizar una red anónima es definir el modelo de amenaza, si creemos que no hay lo que sería anonimato autentico, esto significaría un alto costo de reconocer a alguien. El propósito de esta tecnología I2P es de llegar a comunicar a la personal en un medio arbitrariamente irregular al administrar un buen anonimato, mezclado con un alto tráfico de cobertura realizado por la diferentes actividades de los clientes que deseen menos anonimato, como podemos observar en la figura 1 (Proyecto de Internet Invisible, 2010).

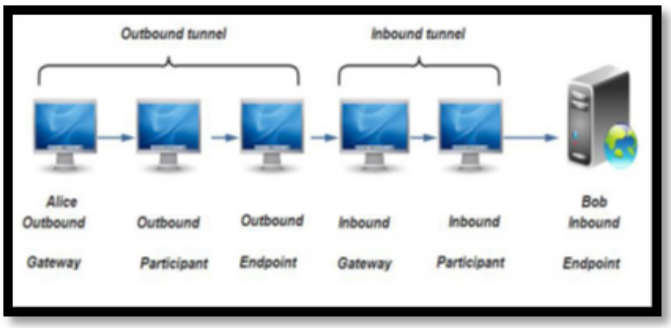

Figura 1. Función de I2P.

Fuente: Proyecto de Internet Invisible (2010).

Por esta razón es que se requiere un sistema que tenga un buen soporte

En las comunicaciones anónimas, cada una tiene su propia razón. Ya que existe algunos proyectos en internet, pero no se encuentra ninguno que satisfagan nuestras necesidades o la amenaza (Proyecto de Internet Invisible, 2010).

Se encuentra estructurada en los conceptos de túneles entrantes y salientes, lo cual brinda una facilidad para su adaptación en programas preexistentes de la red I2P. Cada túnel está formado por una secuencia de nodos padres, los cuales traslada la información en un sentido unidireccional (Mejía Barrera, et al., 2014).

Por ejemplo, la primera vez que un cliente desea enviarle información a otro cliente, ambos hacen una consulta completamente distribuida, *Base de dato de red* una tabla de hash distribuida (DHT) con una estructura adaptada en algoritmo Kademlia como nos podemos apreciar en la figura 2 (Mejía Barrera, el al., 2014).

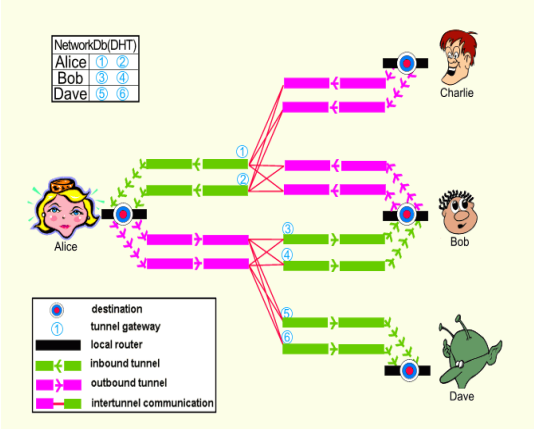

Figura 2. Ejemplo de tipología de red I2P.

Fuente: Proyecto de Internet Invisible (2010).

Para el desarrollo de la investigación se estimó una forma cualitativa – cuantitativa de un proyecto investigativo de campo, como se trata de una investigación aplicada para comprender y resolver varias situaciones, necesidad o problema de un contexto determinado, permite tener datos más relevantes a ser analizado, adoptando nuevos conocimientos y criterios que ayuden al estudio de la situación y facilite las respectivas necesidades para otorgar una solución.

El proyecto de investigación es de tipo descriptivo por que describe sus características, detalles y causas más relevantes del problema, con lo cual nos permite los eventos de estudio, procesos o la oferta de producto a estudiar.

Se ha realizado varios tipos de estudio como la observación y encuesta, para tabular la información necesaria.

Es por esta razón que se utiliza un método técnico más efectivo para obtener una respuesta eficaz.

Para la obtención de la información, se ha concluido con elaboración de encuestas, para su realización se ha contactado personal consideradas para el desarrollo de este trabajo y fueron entregadas a los encuestadores de manera presencial dando un plazo de tiempo para que sean llenadas y entregadas respectiva información sea esta por e-mail o personalmente de ser necesario

Las encuestas se la realizaron a los estudiantes de la facultad de ciencias Matemática y Física de la carrera de Sistema y Networking, la cual ellos se lucrarán de esta propuesta, también será aplicada la universidad de las diferentes facultades que posee la universidad de Guayaquil para indicar los beneficios que obtendrán.

Una vez finalizada las encuesta y aplicado en cada instrumento de la investigación, se efectúa de forma manual la tabulación de la documentación, realizada por los estudiantes, docentes y trabajadores de la carrera de Telecomunicación y Networking. Luego se procede a realizar un análisis e interpretación de la información de los datos estadístico para dar respuesta a los objetivos de la investigación.

Con el presente estudio se hace referencia al estudio metodológico detallado en dicho trabajo. El proyecto es factible ya que se encuentra avalado por la carrera de Networking y Telecomunicación, quienes han permitido realizar la implementación con el objetivo de que podamos ejecutar nuestra propuesta metodológica.

CONCLUSIONES

Con el surgimiento de la tecnología I2P se puede lograr la optimación de mejor manera, la seguridad del envío de información por medio de la red que en la actualidad es un recurso que se puede optimizar mediante su aceptación ya que los involucrados en el proceso del anonimato se encuentra dispuesto a cambios los que permite optimizar la información que utilicen para el envío de información por medio de la red. Esta propuesta metodológica se encuentra diseñada de tal forma que la tecnología I2P se puede adecuar a su estructura interna para ser utilizada en cualquier equipo.

REFERENCIAS BIBLIOGRÁFICAS

Brezo Fernández, F., & Rubio Viñuela, Y. (2011). Herramientas de apoyo a la infraestructura tecnológica de los grupos organizados que operan en la red. Cuadernos de la Guardia Civil: Revista de seguridad pública, 50, 27-47. Recuperado de https://dialnet.unirioja.es/ejemplar/410664

De Luz, S. (2012). I2P: red segura y anónima para navegar, chatear y descargar archivos. Recuperado de https://www.redeszone.net/2012/09/07/i2p-red-segura-y-anonima-para-navegar-chatear-y-descargar-archivos/

Hurtado de Barrera, J. (2010). Metodología de la Investigación Holística. Guía para la compresión holística de la ciencia. Cuarta Edición. Bogotá: Magisterio.

Mejía Barrera, Y. P., & Peralta Palacios, E. J. (2014). Evaluación de herramientas para la protección de las comunicaciones en redes sociales y dispositivos móviles . tesis para optar al título de Ingeniero en Telemática. León: Universidad Nacional Autónoma de Nicaragua.

Proyecto de Internet Invisible. (2010). I2P: Un sistema escalable para las comunicaciones anónimas. Recuperado de https://geti2p.net/es/docs/how/tech-intro

Sánchez Cañestro, A. (2015). MISTIC Programas de vigilancia masiva y contramedidas aplicables. Rambla del Poblenou: Universitat Oberta de Catalunya