UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTORES:
JAVIER MAURICIO BRIONES GARATE
HÉCTOR LUÍS HINOJOSA CHAMBA

TUTOR:
ING. MARLON ALTAMIRANO DI LUCA, MSIA.

GUAYAQUIL – ECUADOR
2017

REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER.		
	REVISORES:	
INSTITUCIÓN: Universidad de Guayaquil	**FACULTAD:** Ciencias Matemáticas y Físicas	
CARRERA: Ingeniería en Networking y Telecomunicaciones		
FECHA DE PUBLICACIÓN:	**N° DE PÁGS.:**	
ÁREA TEMÁTICA: Redes		
PALABRAS CLAVES: seguridad – redundancia - factibilidad		
RESUMEN:		
N° DE REGISTRO:	**N° DE CLASIFICACIÓN:** **Nº**	
DIRECCIÓN URL:		
ADJUNTO PDF	[X] **SI**	[ ] **NO**
CONTACTO CON AUTOR: Javier Mauricio Briones Garate Héctor Luís Hinojosa Chamba	**TELÉFONO:** 099047384 0986868441	**E-MAIL:** Javier-music_master@hotmail.com hhinojosa19@hotmail.com
CONTACTO DE LA INSTITUCIÓN:	**NOMBRE:**	
	TELÉFONO:	

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de campo, con el tema **ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER** elaborado por los **Srs. Javier Mauricio Briones Garate y Héctor Luís Hinojosa Chamba**, egresados de la Carrera de Ingeniería en Networking y Telecomunicaciones, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

……

Ing. Marlon Altamirano Di Luca, MSIA.

TUTOR

DEDICATORIA

Esta monografía está dedicada a mi madre Rosario Garate ya que gracias a ella he podido culminar esta etapa y poder aportar con mis conocimientos. También dedico a mis abuelos ya que con ellos sigo siendo una persona de bien.

Briones Garate Javier Mauricio

DEDICATORIA

Esta tesis está dedicada a mi familia por el aliento y motivación a lo largo de mi vida personal y profesional.
Así también a los docentes de cada área por su esfuerzo, dedicación y paciencia.

Hinojosa Chamba Héctor Luis

AGRADECIMIENTO

Agradezco a mi familia por el aliento y motivación a lo largo de mi vida personal y profesional.
Así también a los docentes de cada área por su esfuerzo, dedicación y paciencia.

Briones Garate Javier Mauricio

AGRADECIMIENTO

Agradezco a mis compañeros de universidad por acompañarme en esta aventura profesional y compartir cada momento en nuestra carrera.

Quiero agradecer a mis madres Carmen y Olga por su esfuerzo y dedicación que me ha permitido tener una excelente educación y que será la base para mi futuro.

Hinojosa Chamba Héctor Luis

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, Sc.
DECANO DE LA FACULTAD
CIENCIAS MATEMATICAS Y
FISICAS

Ing. Harry Luna Aveiga, Mgs.
DIRECTOR
CARRERA DEINGENERIA EN
NETWORKING Y
TELECOMUNICACIONES

Ing. Marlon Altamirano DiLuca,
MSIA.
DIRECTOR DEL PROYECTO DE
TITULACIÓN

Lic. Ruth Elizabeth Paredes S.
PROFESOR DEL ÁREA -
TRIBUNAL

Ing. Eduardo Flores Moran
PROFESOR DEL ÁREA - TRIBUNAL

Ab. Juan Chávez Atocha, Esp.
SECRETARIO TITULAR

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL"

JAVIER BRIONES GARATE

FIRMA

HÉCTOR HINOJOSA CHAMBA

FIRMA

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER.

Proyecto de Tesis de Grado que se presenta como requisito para optar por el título de INGENIERO en Networking y Telecomunicaciones

Autores:

Javier Mauricio Briones Garate

C.I. 09303804-0

Héctor Luís Hinojosa Chamba

C.I. 092635224-6

Tutor: Ing. Marlon Altamirano Di Luca, MSc.

Guayaquil, Noviembre del 2016

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor de Tesis de Grado, nombrado por el Departamento de Investigación, Desarrollo Tecnológico y Educación Continua de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil,

CERTIFICO:

Que he analizado el Proyecto de Grado presentado por los egresados Javier Mauricio Briones Garate y Héctor Luís Hinojosa Chamba, como requisito previo para optar por el título de Ingeniero cuyo problema es: **ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER**, considero aprobado el trabajo en su totalidad.

Presentado por:

Javier Mauricio Briones Garate	**C.I. 09303804-0**
Héctor Luís Hinojosa Chamba	**C.I. 092635224-6**

Tutor: Ing. Marlon Altamirano, MSIA.

Guayaquil, Noviembre del 2016

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

Nombre Alumno: Héctor Luís Hinojosa Chamba	
Dirección: Ciudad Victoria 2 Mz. 4537 Sl. 1A2	
Teléfono: 0986868441	**E-mail:** hhinojosa19@hotmail.com

Nombre Alumno: Javier Mauricio Briones Garate	
Dirección: Buenos Aires 716 y Oconnor	
Teléfono: 0991047384	**E-mail:** Javier-music_master@hotmail.com

Facultad: Ciencias Matemáticas y Físicas
Carrera: Ingeniería en Networking y telecomunicaciones
Proyecto de titulación al que opta:
Profesor tutor: Ing. Marlon Altamirano, MSIA.

Título del Proyecto de titulación: Análisis de las ventajas del uso del protocolo OpenDHT para la descentralización de comunicaciones Peer-to-Peer.

Tema del Proyecto de Titulación: Análisis, Investigación

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica:

Inmediata	**X**	Después de 1 año	

Firma Alumno: Héctor Luís Hinojosa Chamba

3. Forma de envío:

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM	**X**	CDROM	

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER.

Proyecto de Tesis de Grado que se presenta como requisito para optar por el título de INGENIERO en Networking y Telecomunicaciones

Autores:

Javier Mauricio Briones Garate

C.I. 09303804-0

Héctor Luís Hinojosa Chamba

C.I. 092635224-6

Tutor: Ing. Marlon Altamirano, MSc.

Guayaquil, Julio del 2017

INDICE GENERAL

Contenido

INDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ABREVIATURAS

API: Según sus siglas en inglés, Application Programming Interface, Interfaz de Programación de Aplicaciones, es un grupo de procedimientos que un programa de PC llama para acceder a un servicio específico.

AUI: Asociación de usuarios de Internet.

BIT: Dígito Binario o por sus siglas en inglés – Binary Digit,, es la unidad mínima de almacenamiento y procesamiento de la información, puede tomar dos únicos valores: 0 o 1.

CRC: Según sus siglas en inglés – Cyclic Redundancy Check, es un sistema de verificación de integridad de datos.

DLL: Según sus siglas en inglés - Dynamic Link Library, Librería de Concatenación Dinámica, son rutinas (Librerías) que mejoran la compatibilidad entre el hardware y las aplicaciones. Generalmente son escritas de modo que puedan ser usadas simultáneamente por varios programas.

FTP: Según sus siglas en inglés - File Transfer Protocol, Protocolo de Transferencia de Archivos para subir y descargar archivos de un sistema a otro, FTP genera un enlace TCP con el sistema objetivo, para el intercambio de mensajes de control.

GII: Infraestructura Global de Información.

GSM: Sistema Global de Comunicaciones Móviles.

GSP: Según sus siglas en inglés - Government Security Program, iniciativa por la cual Microsoft ofrece a los Gobiernos acceso controlado al código fuente de Windows.

IRQ: Según sus siglas en inglés - InterruptRequest, Requerimiento de Interrupción, interrupción de hardware en un PC (Personal Computer). Las interrupciones son generadas por dispositivos periféricos como módems, NICs (Network Interface Cards). Dos dispositivos no pueden utilizar la misma línea a no ser que éstas sean programadas para interactuar, de ahí que cuando coinciden tengamos problemas en el PC.

ITU: Unión Internacional de Telecomunicaciones.

NAP: Según sus siglas en inglés - Network Access Point, Punto de Acceso a la Red, son los puntos principales de acceso a grandes redes como Internet o el VBNS (Very-high-speed Backbone Network Service).

NCSA: Centro Nacional de Aplicaciones de Supercomputación.

PPP: Según sus siglas en inglés - Point-to-Point Protocol, Protocolo Punto a Punto, Protocolo de comunicaciones serial utilizado en enlaces de redes, también es como se mide la resolución de un escáner o impresora (Punto por Pulgada).

UDP: Según sus siglas en inglés - UserDatagramProtocol, Protocolo de Datagramas de Usuario, protocolo de transporte que se utiliza como parte de TCP/IP. Provee un servicio sin conexión para procedimientos en el nivel de aplicación. No garantiza entrega, (lo que si hace el TCP), ni preservación de secuencia ni protección contra duplicación.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS

CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER.

Autores:

Javier Mauricio Briones Garate

C.I. 09303804-0

Héctor Luís Hinojosa Chamba

C.I. 092635224-6

Tutor: Ing. Marlon Altamirano, MSc.

RESUMEN

El contenido de este trabajo investigativo tiene como objetivo demostrar las características de la tabla de hash distribuida (DHT) y cómo ha jugado un papel importante en la mejora de conectividad de sistemas y aplicaciones, especialmente en entornos distribuidos, centralizados y descentralizados a gran escala, siendo así un desafío en la arquitectura de sistemas a gran escala, específicamente denominado modelo cliente/servidor normal (modelo C/S).

Los sistemas centralizados de gran escala presentan un inconveniente denominado en el área de informática como "saturación de red" que a diferencia del sistema descentralizado, ejemplificado por el modelo peer-to-peer (P2P), aprovecha los recursos distribuidos a través de una lista de nodos. Al mismo tiempo, es considerado una solución viable para utilizar la capacidad de todos los

nodos de una manera eficiente y proporcionar una mayor robustez en el campo de la seguridad de la información. Para cumplir con estos requisitos se desarrolló una tecnología llamada DHT. Con dicha tecnología, una vez distribuidos los recursos son de fácil administración lo que permite al usuario acceder de forma segura al sistema con sólo conocer parte del mismo. La elegancia de DHT es la practicidad de su funcionalidad, pues proporciona únicamente dos operaciones básicas incluyendo: (i) datos GET de DHT y (ii) datos PUT en DHT. En efecto, dada su simplicidad, DHT permite interactuar con gran variedad de aplicaciones proporcionando seguridad y alta eficiencia, especialmente en sistemas a gran escala.

Finalmente, muchas aplicaciones basadas en DHT han propuesto mejorar el sistema P2P mediante actualizaciones de su lenguaje de programación que se han centrado principalmente en el aspecto de la eficacia de redes de alta escala con una mayor atención a plataformas y aplicaciones, como multicast, anycast, y otros sistemas de archivos distribuidos.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS

CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER.

Autores:

Javier Mauricio Briones Garate

C.I. 09303804-0

Héctor Luís Hinojosa Chamba

C.I. 092635224-6

Tutor: Ing. Marlon Altamirano, MSc.

ABSTRACT

The purpose of this research is to demonstrate the characteristics of the Distributed Hash Table (DHT) and how it has played an important role in improving the connectivity of Systems and Applications, especially in distributed, centralized and decentralized environments on a large scale, Thusbeing a challenge in the large-scale system architecture, specifically called the normal client / server model (C / S model). Large-scale centralized systems have a draw back called in the area of computing as "network saturation" which, unlike the decentralized system, exemplified by the peer-to-peer (P2P) model, takes advantage of resources distributed through a list of nodes. At the same time, it is considered a viable solution to use the capacity of all nodes in an efficient way and to provide a greater robustness in the field of information security. To meet these requirements, a

technology called DHT was developed. With this technology, once distributed resources are easy to administer which allows the user to securely access the system with only knowing part of it. The elegance of DHT is the practicality of its functionality, as it provides only two basic operations including: (i) DHT GET data and (ii) DHT data in DHT. Indeed, given its simplicity, DHT allows to interact with a wide variety of applications providing security and high efficiency, especially in large scale systems.

Finally, many DHT-based applications have proposed upgrading the P2P system through updates to its programming language that have focused primarily on the efficacy aspect of high-scale networks with increased attention to platforms and applications such as multicast, any cast, and some other distributed file systems.

INTRODUCCIÓN

En la última década, se ha realizado un trabajo extenso para DHT, mediante pruebas de campo y aportaciones de diferentes investigadores que han propuesto numerosas mejoras y variantes de DHT que nos permiten, en teoría, gestionar los recursos en muchos tipos de estructuras informáticas, ya sean sistemas distribuidos o centralizados de información, proporcionando abundantes probabilidades de mejoras para diferentes maneras de construir un sistema tolerante a fallos y que permita un nivel de encriptación alto para mantener seguros datos críticos.[1]

Con esta idea, muchas plataformas de DHT que han sido construidas, pueden ser consideradas como un puente que transforma DHT de la teoría a la práctica, debido a que por medio de su implementación, permite resolver muchos problemas prácticos como el balanceo de carga, múltiples réplicas de comunicación, coherencia del sistema a analizar el tráfico de red, etc. De esta forma, DHT otorga diferentes maneras de encontrar las fortalezas y debilidades de un sistema distribuido.[1]

Además, se proponen muchas aplicaciones basadas en DHT tales como multicast, anycast, sistemas de archivos distribuidos, búsqueda, almacenamiento, red de distribución de contenido, archivo, compartir y comunicar datos en el momento en que el administrador del sistema lo requiera de forma rápida, controlada y eficaz.

DHT ha empezado a afianzarse como parte de las redes P2P, por medio de datos obtenidos por varios estudios de la propuesta investigativa donde todas las variantes (de DHT) se clasificarían por topologías de funcionalidad que complementan las comunicaciones P2P por medio de mejoras en la compilación de robustez y seguridad. Sin embargo, en estas aportaciones los autores ignoraron muchas de las plataformas DHT y aplicaciones que son muy importantes, especialmente en el área industrial. Es por eso que este material de estudio estará compuesto por cinco capítulos.[1]

En el capítulo uno se encuentra elaborado el planteamiento de estudio sobre Open DHT como solución de ambientes descentralizados basados en la comunicación P2P, incluyendo la motivación del planteamiento de estudio, [1] presentando los motivos que inspiran el trabajo investigativo así como la definición de objetivos y alcances que tendrá el desarrollo del tema investigación, conceptos básicos y la terminología de los sistemas P2P estructuradas, proporcionando una estructura

lógica y analítica de las razones detrás de la expresión "sistema P2P estructurada" y centrar la discusión sobre las propiedades teóricas y problemas prácticos de tales sistemas.

Dentro del capítulo dos se estudian siete variantes de DHT y se comparan en muchos aspectos, como son: algoritmos de cifrado, de enrutamiento y verificación. DHT con 15 plataformas diferentes y aplicaciones que pueden ser construidas e implementadas como soluciones a ambientes de alta escala y tráfico de información. Además de las ventajas de DHT sobre estas aplicaciones, incluyen ejemplos concretos de diseños para DHTs clásicos existentes, en los cuales se enfoca a estructuras de topología de red que utilizan DHT, facilitando una introducción básica a los sistemas P2P y problemas de su diseño.

Actualmente, existen muchos trabajos en diseños y técnicas concretas P2P, en sus modelos básicos, módulos de algoritmos, propiedades teóricas y experimentales que nos motivan estudiar conclusiones del caso de estudio, haciendo referencia a DHT. La mayoría de los logros teóricos y prácticos esenciales ya se resumen en diversas encuestas y libros.

En el capítulo tres hacemos referencia a dos tipos de plataformas: plataforma académica y de código abierto y plataforma comercial, incluyendo datos sobre encuestas preparadas para la obtención de información vital que identifica a DHT como solución factible ante problemáticas de “cuello de botella” en la gestión de información.

Finalmente, en el capítulo cuatro se encuentra el estudio de factibilidad, análisis de los datos obtenidos a lo largo del desarrollo de la propuesta investigativa, además de las mejoras consolidadas para mejora del sistema DHT y las diferentes distribuciones que presenta actualmente.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

LA FALTA DE CIFRADO DE LA INFORMACIÓN POR MEDIO DE UN PROTOCOLO DE SEGURIDAD PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER TO PEER.

Ubicación del problema en un contexto

En los últimos años, se han generado varios análisis y estudios sobre los sistemas de la tabla de Hash distribuida (DHT) ya que juega un papel importante en la distribución de Sistemas y aplicaciones, especialmente en entornos distribuidos a gran escala en el cliente y el servidor normal (modelo C / S) .
Debido a que el servidor central está a cargo de la mayoría de los recursos, se convierte en la parte más importante, así como el cuello de botella y punto débil del sistema por la cual los atacantes se aprovechan de las vulnerabilidades que presenta la plataforma, explotándolas para la captura de mensajes y claves y a su vez usarlas para beneficio propio descifrando de una manera fácil los mismos paquetes que circulan por la red.
Por el contrario, el modelo distribuido es el Peer-to-peer (P2P), el cual asigna los recursos en los nodos; además el modelo distribuido proporciona una mayor robustez y utiliza más eficientemente todos los Peers, mientras que los recursos de los clientes están inactivos en modo C / S., en distribuidos un problema clave es cómo administrar los recursos de manera eficiente.

Las redes sociales en la actualidad son una de las formas más importantes de la comunicación a nivel de todo el mundo, pero a su vez presentan agujeros de seguridad y esto causa que su nivel de competitividad disminuya si no es capaz de seguir el ritmo de aumento de las actividades del usuario y la implementación de un protocolo que tenga la capacidad de cifrar de una manera segura las

comunicaciones P2P, además que posea una alta escalabilidad de encriptación de claves proporcionadas por el sistema y lleve una mejor eficiencia en el momento de aplicar este tipo de protocolo de seguridad en las aplicaciones del mundo moderno, pero para el mejor rendimiento que uno necesita es determinar dónde es mejor en todos los sistemas de comunicación para poner los datos, almacenándolos y a su vez evitando el acceso a usuarios no autorizados.

Es un tema particularmente importante en los sistemas a gran escala, OpenDHT aborda el problema y promueve el desarrollo de P2P grandemente. OpenDHT es un diseño simple y elegante para sistemas distribuidos. Proporciona el funcionamiento como una tabla hash para tratar con los datos distribuidos. No requiere de un servidor central y trata todos los nodos OpenDHT en el sistema distribuido por igual.

Mientras tanto, OpenDHT hereda las grandes propiedades de la tabla hash (por ejemplo, localizar y buscar un elemento con alta eficiencia). Proporciona un espacio clave global y abstracto (a menudo denominado espacio OpenDHT),

Al igual que en la tabla hash, cualquier dato en OpenDHT podría ser tratado como una dupla .K; V /, donde K denota la clave que se mapea de los datos mediante un hash Función y V denota los datos originales. Cada nodo también tiene una llave llamada ID del nodo en el espacio OpenDHT. Así, todos los datos y nodos en un sistema distribuido pueden ser consistentemente mapeados en el espacio OpenDHT.

El espacio DHT se divide en ranuras, cada nodo en un sistema OpenDHT mantiene los datos que se asignan en la ranura de este nodo. Como resultado de su diseño simple y elegante, OpenDHT tiene dos operaciones primitivas que son : Put, es una función que pone los datos V en el espacio OpenDHT con una clave K. Get, es una función que obtiene los datos originales utilizando una clave dada K. Aunque extremadamente simple, estos dos primitivos son adecuados para una gran variedad de aplicaciones y proporcionan buena robustez y alta eficiencia, especialmente en sistemas a gran escala a diferencia de otros protocolos. [2]

Situación Conflicto. Nudos Críticos

La problemática surge porque la mayoría de los protocolos que se encargan de cifrado de comunicaciones P2P dependen de un servidor central que se encargue de todas las tareas y peticiones de los usuarios, además gestiona todos los recursos del sistema convirtiéndolo en la parte más importante, presentado los riesgos a sufrir mediante un ataque informático en el cual los atacantes buscan vulnerar los datos transmitidos por los usuarios.

Es un sistema de almacenamiento distribuido, donde los datos se dividen en una serie de servidores, los datos también pueden ser replicados para proporcionar un alto grado de disponibilidad en caso de fallos. Mientras que la partición de datos y la replicación es un problema bien conocido en la literatura de los sistemas de bases de datos.

Han demostrado que las consultas distribuidas de registros de datos pequeños reducen el rendimiento en comparación con las consultas locales. Por lo tanto la localidad social debe tenerse en cuenta al diseñar un almacenamiento distribuido.[3]

Causas y Consecuencias del Problema

TABLA 1 CAUSAS Y CONSECUENCIAS

Dependencia de un servidor central para gestionar los recursos necesarios e importantes para los usuarios.	Surge como consecuencia que dicho servidor que gestiona recursos y tareas de usuarios se vuelva un punto débil donde los atacantes pueden violentar la confidencialidad e integridad de la información.
La falta de conocimiento sobre protocolos de seguridad para la descentralización de las comunicaciones P2P	Los atacantes maliciosos ocasionan una mayor intersección de los datos sensibles por medio de ataques hombre en el medio.

Los sistemas de descentralización de comunicaciones P2P tienen la funcionalidad de replicar los datos y particionarlos.	Reduce el rendimiento a las consultas de datos realizadas por los usuarios causando un colapsando en el servidor central.
En los sistemas distribuidos permiten la administración de recursos para las peticiones de los usuarios al servidor.	La clave es la difícil administración de los recursos que nos proporciona la plataforma para evitar que el servidor central no sufra una caída del enlace con los usuarios.

Autores: Javier Briones-Héctor Hinojosa

Fuente: Trabajo de Investigación

Delimitación del problema

Los siguientes términos que se adaptan al proyecto de investigación son:

- **CAMPO:** SEGURIDADES DE REDES DE COMUNICACIÓN (SEGURIDAD INFORMATICA).
- **ÁREA:** CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIOMES
- **ASPECTO:** PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN
- **TEMA:** TEMA: “ANÁLISIS DE LAS VENTAJAS DEL USO DEL PROTOCOLO OPENDHT PARA LA DESCENTRALIZACIÓN DE COMUNICACIONES PEER-TO-PEER.”.

Formulación del problema

¿En qué medida incide el protocolo OpenDHT para el mejoramiento del traslado de información y en qué sectores puede beneficiar su utilización?

Evaluación del Problema

En nuestro problema de investigación se han seleccionado 6 aspectos principales para la evaluación del problema.

Los aspectos generales de evaluación son:

Delimitado: La problemática demuestra que los protocolos similares a OpenDHT reducen el rendimiento de los sistemas de mensajería instantánea, servicios de correo electrónico, servicios transaccionales y de más aplicaciones incorporadas en las organizaciones ubicadas en la ciudad de Guayaquil.

Concreto: La problemática redacta que los protocolos similares a OpenDHT dependen de un servidor central que gestione recurso para el usuario convirtiéndolo en un punto débil a ataques informáticos y la falta de conocimiento del protocolo mencionado anteriormente.

Relevante: Una de las observaciones que se pudo identificar que los protocolos similares a OpenDHT dependen de un servidor central que gestione las tareas, recursos y peticiones de los usuarios donde dicho servidor se convierte en un punto importante pero además se vuelve en el punto más débil donde los cracker pueden aprovechar de las vulnerabilidades presente ocasionado el colapsamiento del servidor inundándolo de tantas peticiones e interceptando los paquetes que circulan dentro y fuera de la red.

Además otros de los indicadores que se verificó es la falta de conocimiento sobre protocolos de cifrado para comunicaciones P2P, haciendo que estos sistemas implementados sean vulnerables a ataques cibernéticos por no tener conocimiento en protocolos de encriptación robusta.

Original: El proyecto de investigación a desarrollar sobre el protocolo OpenDHT en la descentralización en las comunicaciones P2P demuestra la originalidad, por la cual los investigadores no se han percatado que si existe un protocolo de cifrado robusto en las transmisión de la información que pasa por medio de un canal de comunicación y que certifica la seguridad de los datos de los usuarios.

Factible: En el análisis a desarrollar sobre las ventajas del protocolo Open DHT demuestra la factibilidad; las empresas que utilizan sistemas de mensajería, correo electrónico y demás aplicaciones integradas podrán verificar que la información esté cifrada de una manera segura y además el mismo protocolo provee un alto rendimiento, escalabilidad, robustez en la transferencia de datos y eficiencia garantizando la seguridad de la información de las compañía que tienen implementado este tipo de servicios mencionados anteriormente en su infraestructura de red.

Identifica los productos esperados: La investigación a desarrollar contribuye con solucionas alternativas porque se dará a conocer la funcionalidad del protocolo OpenDHT y la manera cómo cifra los datos protegiendo la confidencialidad, integridad y disponibilidad de la información aplicando algoritmos de encriptación fuertes a diferencia de otros protocolos.

Alcances del Problema

Los alcances del problema planteado nos ayudaran con alternativas de solución utilizando el protocolo OpenDHT para el cifrado robusto en las comunicaciones P2P logrando así plantear las medidas de seguridad adecuadas para reducir el nivel de riesgo y amenazas hacia la información de carácter confidencial e íntegro que manejan las organizaciones; además, el uso de este protocolo de seguridad nos proporciona un sistema tolerante a fallo para que las peticiones que demandan los usuarios no afecten al servidor cuando existe un colapsamiento en la red P2P; y la redundancia que viene integrada en el protocolo en mención, nos facilita a que cuando existe una caída en un nodo de la red éste se vaya por otro camino dando continuidad al servicio que se está ejecutando en la red.

OBJETIVOS DE LA INVESTIGACION

Objetivo General

- Realizar un estudio del protocolo OpenDHT para la descentralización de comunicaciones P2P implementado el equilibrio de carga y la integridad de los datos estableciendo el rendimiento en almacenamiento de la información y la recuperación completa de los datos manteniendo un gran escalabilidad y robustez del sistema.

Objetivos Específicos

- Describir las características y beneficios de un sistema tolerante a fallos para la interconexión de nodos de forma continua.

- Establecer redundancia para un mejor control de los datos transmitidos por el protocolo OpenDHT.

- Determinar el uso de tablas hash distribuidas para el enrutamientos de contraseñas estructurado para mejorar la seguridad de la información.

- Plantear un esquema de almacenamiento de contenido direccionable para la ocultación de archivos confidenciales.

- Seleccionar sistemas criptográficos compatibles con el protocolo OpenDHT para el cifrado de la información y almacenamiento en la red.

JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

La investigación a desarrollarse garantiza la seguridad que se va implementar a futuro por medio del protocolo OpenDHT certificando la confidencialidad, integridad y disponibilidad de la información y los activos de gran importancia que manejan las organizaciones, donde se utilizará un sistema de cifrado que encripte

los datos sensibles evitando el acceso a usuarios malintencionados a la información de carácter confidencial, y además el protocolo mencionado, provee una gama de servicios como la escalabilidad, la robustez de la información y la alta eficiencia para el manejo de esta aplicación integrada en las redes P2P.
Las personas beneficiarias serían los usuarios que laboran para las compañías y las mismas tendrán protección de los datos que se transmiten por medio de la red.

Una de las herramientas a utilizar son los sistemas operativos Linux con la integración del lenguaje de programación de JAVA para demostrar la funcionalidad del protocolo OpenDHT y explotar al máximo los servicios que vienen integrado en el mismo por medio del modelo de sistemas de chat en línea en entornos corporativos cliente-servidor.

CAPÍTULO II

MARCO TEÓRICO

SISTEMAS DE CRIPTOGRAFIA UTILIZANDO PROTOLOS DE SEGURIDAD EN INTERNET PARA EL CIFRADO DE INFORMACION CONFIDENCIAL

En la actualidad, las personas que habitan en la ciudad de Guayaquil dependen del servicio de internet cada día para realizar sus actividades diarias y llevar a cabo sus gestiones. Como resultado de esto ha surgido la Internet de las Cosas (IoT) que ha aumentado significativamente los dispositivos conectados a Internet; alcanzando alrededor de 20 mil millones de dispositivos conectados y se espera que llegue a 50 mil millones en 2020. Esto ha creado grandes retos para mantener la seguridad y la privacidad de la información en las comunicaciones P2P, porque la mayoría de los dispositivos se centran en la conectividad y están incluyendo ajustes predeterminados donde la seguridad se ve gravemente afectada por los atacantes maliciosos que violentan la confidencialidad, integridad y disponibilidad de los datos.[4]

En este estudio de investigación, los analistas e ingenieros de seguridad informática presentan los resultados obtenidos por el protocolo de revisión sistemática para establecer el estado actual de seguridad en dispositivos IoT y en las comunicaciones de red de acceso al internet. También en dicho resultado de la revisión, se detectaron las principales preocupaciones, amenazas, ataques, desafíos y algunas contramedidas hacia la privacidad de los datos de los usuarios.[4]

Actualmenteel Internet se ha vuelto indispensable y un servicio de gran importancia en la vida diaria de los habitantes del planeta tierra, día a día se está incrementando su uso prácticamente en todos los ámbitos, conectando una amplia variedad de dispositivos, como: vestibles (wearables), electrodomésticos,

automóviles, dispositivos médicos y una gama de sensores (RFID[1], NFC[2], etc.), entre otros. Lo cual, originó que la cantidad de dispositivos conectados al Internet superara al número de habitantes en el mundo (entre 2008 y 2009), dando como resultado el término “Internet de las cosas” (IoT, por sus siglas en inglés). Este gran incremento en el número de equipos conlleva un gran reto para la seguridad y la privacidad de los datos que son transmitidos por usuarios residenciales y corporativos, ya que por lo general son productos novedosos que ofrecen una funcionalidad específica de poderse comunicar de una manera que el usuario obtenga la movilidad y pueda conectarse en cualquier sitio de una ciudad. Por esto, muchos fabricantes descuidan la seguridad, por tanto, estos equipos se vuelven vulnerables a ataques informáticos, debido a la competencia por llegar primero al mercado para que su producto sea fácil de usar y esto ocasiona una gran puerta hacia los crackers que pueden ocasionar desastres en la información y a los activos de las empresas en general. Por esto las entidades corren el riesgo de sufrir pérdidas económicas debido a que no tienen una buena seguridad informática gestionada, adaptados a protocolos de cifrado actuales.[4]

Un estudio realizado por la compañía HP revela que el 70% de los dispositivos de IoT no cifran sus comunicaciones P2P, el 70% permiten a un atacante identificar las cuentas de usuario válidas, el 60% de los que tienen interfaz de usuario son vulnerables a distintos ataques como secuencias de comandos en sitios cruzados (XSS). Considerando que estos dispositivos recopilan una gran cantidad de información sensible para los usuarios, esto se vuelve un gran riesgo de seguridad.

El objetivo de este estudio es realizar un análisis sobre el estado actual de la seguridad en IoT para mostrar qué problemas existen, cuáles ya se están abordando, cómo se está haciendo e identificar si hay algunos que se están dejando desatendidos.[4]

[1] RFID: Radio Frecuencia a larga distancia
[2] NFC: Radio Frecuencia a corta distancia

En uno de los casos de estudio realizado por los estudiantes de la Universidad Técnica Federico Santa María,en el año 2013 verificaron el estado de la seguridad de las comunicaciones P2P.. Esta investigación muestra que dichas comunicaciones tiene una difusión débil y presenta un criptoanálisis que permite al atacante descifrar cualquier imagen cifrada o información confidencial transmitida por los usuarios con más precisión, propone un ataque de división y conquista, que permite a un actor malicioso recuperar los estados internos de la información transmitida por las personas cuando establecen un canal de comunicación P2P y utilizarlos para cifrar o descifrar cualquier imagen o datos confidenciales. Los resultados experimentales demuestran la eficacia del ataque y la falta de difusión del sistema o la red de internet para la privacidad de los activos y la falta de protocolos criptográficos para tener una muy buena comunicación cifrada. Finalmente, se propone una solución que puede incrementar la seguridad del sistema de comunicación P2P y hacer que el criptoanálisis sea ineficaz.[5]

La seguridad de la información se ha vuelto cada vez más importante para las organizaciones que ofrecen diferentes servicios a la sociedad como por ejemplo salud, finanzas, administración, comercio, comunicaciones personales, etc.
Las entidades que existen en la ciudad Guayaquil buscan analistas de seguridad informática que brinden soluciones de seguridad y cifrado a las tecnologías de la información y comunicación implementadas en las compañías para garantizar la confidencialidad de los activos y, por lo tanto, es necesario implementar mecanismos de protección para la información almacenada o intercambiar para defender los servicios que ofrecen a sus clientes y ellos mismos de ataques activos y pasivos. Los algoritmos de cifrado o protocolos de criptografía son el componente básico de la gama de servicios de seguridad. Los sistemas de cifrado como el OpenDHT utilizados hoy emplean principalmente el álgebra, teoría de números y secuencias aleatorias obtenidas a partir de registros de desplazamiento de retroalimentación lineal.
El uso de funciones caóticas en las comunicaciones P2P es un activo de la investigación, debido a que las propiedades intrínsecas y funciones caóticas tales como la impredecibilidad, la sensibilidad y las condiciones iniciales o parámetros, pueden ser fácilmente requisitos de un criptoanálisis en criptosistemas tales como

confusión o difusión. Además, la implementación de funciones caóticas que puede ser muy eficiente en estas comunicaciones para evitar que los atacantes puedan atentar a la privacidad de los datos.[5]

ANTECEDENTES DEL ESTUDIO

Según los estudiantes del centro de investigación de matemáticas de la unidad de zacatecas en el año 2016 demostraron que el 40.48% de los ataques a las comunicaciones P2P son el rastreo de paquetes, espionaje, intercepción, inyección de mensajes, divulgación no autorizada, ataques a la autenticación de datos, de agujero negro, modificación de ruta, ofuscación, eran realizados por atacantes maliciosos para violentar la privacidad de los datos ocasionándoles daño a la información de los usuarios.[4]

Además los mismos estudiantes mencionan que una amenaza es una cosa o persona que constituye una posible causa de riesgo o perjuicio, para ocasionar desastres en los activos tanto físicos como lógicos de las organizaciones.

Para identificar las amenazas es necesario considerar las características especiales de los dispositivos de IoT, ya que por lo general son dispositivos embebidos que no están pensados para que el usuario modifique las configuraciones o actualice el software. Como resultado del análisis se identificó que la mayor cantidad de amenazas se encuentran en el control de acceso en las comunicaciones P2P (40.74%), mientras que las amenazas a la disponibilidad representan un porcentaje muy bajo (3.70%).[4]

Un estudio demostrado por los estudiantes del departamento de ciencias de la computación e ingeniería de la universidad de Texas en Arlington Estados Unidos en el año 2016 mencionaron que las comunicaciones P2P son vulnerables o susceptibles ataques sybil[3] en los que un atacante crea un gran número de identidades y los utiliza para controlar una fracción sustancial del sistema P2P para el cifrado y descifrado de información de los usuarios.[6]

[3]Ataque Sybil: Es aquel que corrompe un Sistema distribuido por una misma entidad que controla distintas entidades en dicha red.

Los atacantes se unieron para lanzar nuevos ataques de sybil, para asumir los recursos e interrumpir la conectividad para subvertir el funcionamiento del sistema P2P. Tales ataques han demostrado ser bastante intensos creando una problemática en sistemas P2P estructurados en los que se colocan nodos en una tabla hash distribuida utilizando protocolos de criptografía similares a OpenDHT en el popular sistema de intercambio de archivos BitTorrent P2P con millones de usuarios cada uno. Los investigadores han documentado esta vulnerabilidad para tomar las respectivas soluciones de seguridad.[6]
Los sistemas de planos de las redes peer-to-peer (P2P) existentes basados en tablas de hash distribuidas (DHTs) se desempeñan insatisfactoriamente bajo churn debido a su topología no jerárquica. Estas DHTs planas (FDHTs) experimentan un bajo índice de éxito de búsqueda, alta latencia de búsqueda y alto uso de ancho de banda como consecuencia de la presencia de churn[4]. Con esto, exploramos el uso de la DHT jerárquica (HDHT), específicamente el diseño de súper peer, en la mitigación de los efectos del churn y reducción de ataques a las comunicaciones P2P. A nuestro leal saber y entender, somos los primeros en estudiar intensivamente los HDHTs con y sin alto churn a través de herramientas de simulación.[7]

Utilizando el simulador OMNeT ++ y el marco OverSim, analizamos DHTs planas y jerárquicas con y sin churn. Los resultados muestran que los HDHT implementados funcionan más satisfactoriamente y proporcionan un alto índice de seguridad en la redes descentralizadas P2P y con un alto cifrado a la información transmitida por los usuarios que un DHT plano debido a un mejor aislamiento de fallas y tamaños de clúster más pequeños a costa de un mayor tráfico de súper pistas. HDHTs son más estables, ya que tienen mejores proporciones de éxito de búsqueda y consulta de datos en el servidor por parte de los clientes. Son más eficientes, como lo demuestran las latencias de búsqueda más bajas y el menor uso promedio del ancho de banda del nodo. Son más escalables ya que su rendimiento no se degrada significativamente por ataques realizados por crackers para el daño a los datos confidenciales, incluso en población alta, con esto, los

[4]Taza de rechazo o llamada también taza de desgaste se utiliza para la rotación de usuarios en redes peer to peer.

HDHT implementados pueden ser utilizados para aliviar los efectos del churn en las redes móviles.[7]

Hoy en día, muchas aplicaciones distribuidas suelen ser desplegadas a gran escala, incluyendo Grid, motores de búsqueda web y redes de distribución de contenido, y se espera que su escala crezca más en términos de número de máquinas, ubicaciones y dominios administrativos. Esto plantea muchos problemas de escalabilidad relacionados con la escala del entorno en el que se ejecutan. Para abordar explícitamente estos problemas, muchos sistemas distribuidos y servicios cotidianos utilizan superposiciones punto a punto (P2P) para permitir que otras partes del sistema se beneficien de la falla, la tolerancia y escalabilidad de la tecnología P2P. En particular, las tablas de hash distribuidas (DHT), que implementan una interfaz simple de put-and-get a una estructura de datos tipo diccionario, se han utilizado ampliamente para superar las limitaciones actuales asociadas con los componentes centralizados y jerárquicos de los sistemas distribuidos, Gestión, descubrimiento de recursos, programación de trabajos, etc.[8]

Sin embargo, el protocolo DHT presenta una serie de problemas de seguridad en sistemas a gran escala, donde un gran número de usuarios son desconocidos para los administradores (por ejemplo, las redes de escritorio). Esto hace que la detección de comportamientos maliciosos por parte de crackers sea una tarea extremadamente compleja. Como resultado, los atacantes maliciosos pueden interrumpir el sistema de maneras muy peligrosas, llevando al fallo del servicio de enrutamiento, que es catastrófico para cualquier DHT.

Para abordar este problema, introducimos Sophia, una herramienta que robustecerá el protocolo OpenDHT integrándole una nueva técnica de seguridad de cifrado robusto donde los actores maliciosos tendrán dificultad de tener acceso a la privacidad de los datos transmitidos en comunicaciones P2P. Además esta técnica de seguridad avanzada combina el enrutamiento iterativo con la confianza local para implementar un servicio de búsqueda seguro con una sobrecarga casi nula. El aspecto clave para incurrir en cero sobrecargas es el uso de la confianza local.

Con la combinación de Sophia y el protocolo OpenDHT, cada usuario identifica qué entradas de enrutamiento son cooperativas basadas en el éxito y el fracaso de sus propias búsquedas, por lo que no se comparte información de confianza.

Nuestros resultados de simulación demuestran que Sophia y el protocolo de cifrado DHT brindan todas las soluciones de última generación para el enrutamiento seguro en DHTs, tanto en entornos dinámicos estables como dinámicos, e incluso para modelos de amenazas colusorias.[8]

FUNDAMENTACIÓN TEÓRICA

DESARROLLO DEL PROTOCOLO OPENDHT

KADEMLIA DHT

Kademlia es una superposición estructurada por el protocolo OpenDHT, ideada por los investigadores Maymounkov y Mazieres que cuenta con varias aplicaciones y técnicas de cifrado robusto y alta escalabilidad en el sistema distribuido como resultado de usar una de las métricas llamada XOR para blindar la seguridad de los datos al ser transmitida en comunicaciones P2P expresando la cercanía entre identificadores o usuarios legítimos. Por ejemplo, debe tenerse en cuenta que el XOR es una métrica que cumple una operación simétrica, más formalmente que otras métricas integradas en protocolos de cifrado similares, donde el XOR utiliza los parámetros (x, y) para cumplir la operación de cifrado.

El XOR establece una distancia entre los identificadores x-y, por lo que no es difícil de ver que la operación simétrica (∀x), y: d (x, y) = d (y, x) es trivial a esta propiedad, que rinde una consecuencia importante de los nodos de Kademlia y reciben consultas de búsqueda de nodos que también son candidatos para ser insertados en sus propias tablas de enrutamiento. Por lo tanto, los nodos se benefician de los mensajes entrantes para construir y mantener eficientemente sus tablas de enrutamiento.

Otra propiedad interesante consiste en la direccionalidad de la operación XOR, debido a que para cualquier x existe exactamente una y que está a la distancia de la función (d (x, y)). Este hecho asegura que las búsquedas dirigidas a la misma

clave convergen a lo largo del mismo camino, independientemente del nodo fuente del sistema distribuido y esta propiedad se puede explotar eficazmente para el almacenamiento en memoria caché.[8]

SOPHIA DHT

La arquitectura y el funcionamiento de Sophia. Ilustra un ejemplo de cómo Sophia reacciona frente a un fallo de enrutamiento proporcionándole todas las soluciones al fallo de seguridad presente reestableciendo el servicio. El ejemplo muestra la interacción entre los componentes principales de Sophia y la revisión de cada componente en orden de uso. Tras la detección del fallo, el primer paso es que el solicitante aplique una política de confianza para evaluar el comportamiento de encaminamiento de cada salto intermedio. Después de la evaluación, el segundo paso es la actualización de las clasificaciones de confianza asociadas con los saltos intermedios utilizando un algoritmo de cálculo de confianza. Donde la información confidencial de los usuarios se almacenan en el Historial personal (PH).[8]

Una de las ventajas, que posee Sophia es donde asigna un valor a cada encaminador que representa el comportamiento exhibido durante la transacción (por ejemplo, 0 o 1, dependiendo de si un nodo remitió un mensaje correctamente o no). Posteriormente, Sophia actualiza esta información en las entradas correspondientes del PH y finalmente, Sophia ejecuta el algoritmo de confianza para actualizar el valor de comportamiento de enrutamiento de cada nodo. Este proceso de actualización de la información de confidencial se lo observa en el historial de almacenamiento de los datos de los usuarios.[8]

Historia personal del OpenDHT

La Historia Personal (PH) es la principal estructura de datos de la arquitectura Sophia, en ella cada nodo Sophia almacena las calificaciones de confianza para cada usuario conocido.

El PH presenta la misma estructura que una tabla de enrutamiento estándar para cada entrada del PH. El valor de h se toma para que exista al menos un candidato honesto para cada entrada w.h.p.
Por un razonamiento similar a la de otros algoritmos, se puede mostrar Que h = Ω (logN) es suficiente para garantizar esta propiedad. A partir de ahora, nos referiremos a cada entrada del PH.[8]

El protocolo DHTs consiste en muchos pares autónomos que se auto-organizan para la superposición de la red en la parte superior de todo el sistema distribuido a gran escala de grandes redes físicas. DHT define una estructura principal para el espacio de claves y la selección de la mejor ruta a más de las entradas de enrutamiento, pero tienen en común todas las operaciones get y put donde se realizan una sobrecarga a la capa básica de enrutamiento basada en clave.
DHTs se pueden clasificar en determinista y no determinista. En un sistema con la implementación del protocolo de seguridad DHT determinista, consiste que el enrutamiento y las tablas son únicas para el mismo conjunto de nodos. Sin embargo, en un enfoque no determinista de DHT, existe cierta flexibilidad en la selección de las entradas de enrutamiento, de modo que un nodo dado puede presentar varias tablas de enrutamiento válidas para el mismo conjunto de nodos participantes.[8]

TIPOS DE ATAQUES QUE AFECTAN A LA CONFIDENCIALIDAD DE LOS DATOS

ATAQUE HOMBRE EN EL MEDIO (INTERCEPCION DE LOS DATOS)

Un ataque Man in TheMiddle (Hombre en el Medio) en diferentes sistemas operativos es aquel que intercepta la comunicación entre un emisor y un receptor capturando los paquetes que pasan por la red a su vez descifrándolos por los atacantes para violar la privacidad de los datos. Una de las herramientas más populares para realizar este tipo de ataque es la herramienta ettercap que nos permite interceptar todos los paquetes que circulan por toda la red inalámbrica o de área local.[9]

GRAFICO 1 ATAQUE MAN IN THE MIDDLE

Fuente:http://www.dragonjar.org/man-in-the-middle-ataque-y-deteccion.xhtml

Autor: Jaime Andrés Restrepo

ANALIZADORES DE TRAFICO (SNIFFER)

La captura de datos es importante para algunas aplicaciones críticas de la red, como el diagnóstico de la red y la investigación criminal.

En las redes inalámbricas multicanal, el desafío fundamental para la captura de datos es cómo asignar canales de operación a los sniffers inalámbricos. Los enfoques existentes hacen algunas suposiciones poco prácticas, como el conocimiento previo sobre el tráfico de red y las condiciones perfectas de captura de datos.

En un estudio, los investigadores descubrieron que la asignación de canales de sniffers en escenarios de múltiples saltos, especialmente el despliegue de redundancia, permite a los sniffers múltiples monitorear un tráfico. Este es una entrada de acceso a los atacantes maliciosos para combinar sus técnicas de ataques a un sistema combinatorio de bandoleros múltiples (MAB), y a su vez puedan los mismos violentar la confidencialidad de los datos.[10]

La captura de datos es un enfoque importante para evaluar el rendimiento de la red, que se ha adoptado en diversas aplicaciones como la supervisión del tráfico, la detección de actividades maliciosas, etc.

Para recopilar la información detallada de PHY / MAC, se ha propuesto un marco de monitoreo pasivo para un conjunto de dispositivos de hardware dedicados, llamados sniffers inalámbricos. Los inhaladores son desplegados para capturar las señales inalámbricas en una zona donde se propaga la señal inalámbrica. Debido a esto, la información recopilada puede analizarse de forma centralizada o distributiva.

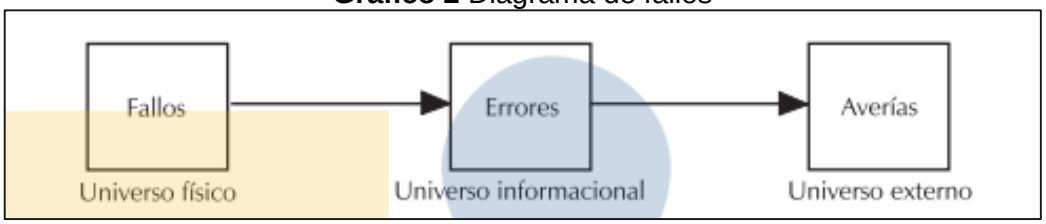
Este marco de monitoreo basado en rastreos ha atraído especialmente en los trabajos inalámbricos multicanal, como WLAN, redes inalámbricas de malla, redes de radio cognitivas. Debido al menor número de sniffers inalámbricos, así como la capacidad de captura limitada, un desafío técnico fundamental es cómo asignar los canales de trabajo para un número limitado de sniffers, es decir, el problema de asignación de canal sniffers, a fin de maximizar la cantidad total de Información recogida.[10]

Sistemas tolerantes a fallos

El fallo en un sistema es cualquier defecto físico o lógico de cualquier componente de hardware o software.

Un sistema puede fallar cuando existe variación de las funciones del mismo, debido a perturbaciones externas tales como la temperatura u ondas electromagnéticas. Un error es el resultado de un fallo o este error es la consecuencia de un fallo en el sistema.[11]

Grafico 2 Diagrama de fallos



Fuente:https://www.infor.uva.es/~bastida/Arquitecturas%20Avanzadas/Tolerant.pdf

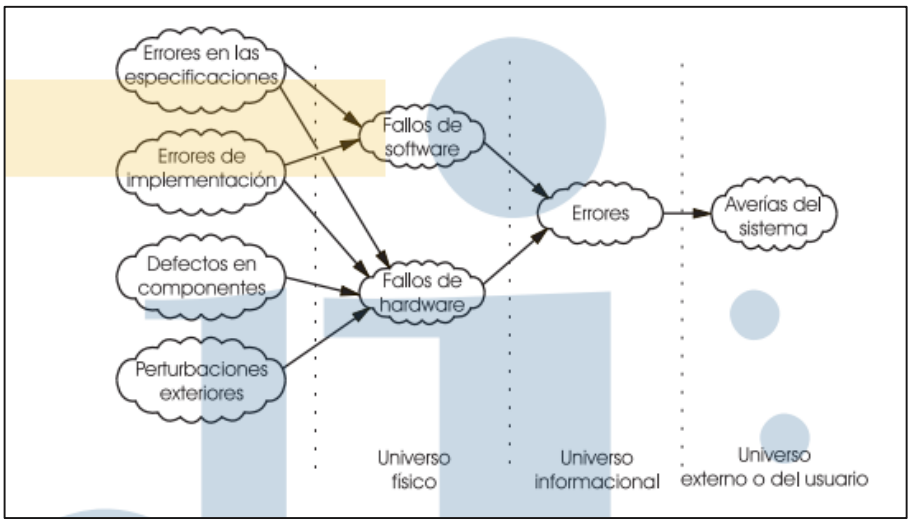
Autor: Universidad de Valladolid

Si un error causa un funcionamiento incorrecto del sistema desde el punto de vista externo, esto quiere decir que las consecuencias del fallo trascienden al exterior del sistema.[11]

Causas de los fallos

Para buscar las causas de los sistemas que contienen algún fallo, se analiza todo el proceso seguido desde el diseño del sistema hasta su explotación pasando por su implementación. Mediante este análisis podemos encontrar el origen de los fallos.[11]

Grafico 3 Características de los fallos



Fuente:https://www.infor.uva.es/~bastida/Arquitecturas%20Avanzadas/Tolerant.pdf

Autor: Universidad de Valladolid

Caracterización de los fallos

Los fallos se pueden caracterizar de la siguiente manera: causa, naturaleza, duración, extensión variabilidad.[11]

- Las causas de los fallos pueden ser múltiples en el momento del diseño y el proceso de su implementación.
- La naturaleza de los fallos es la que especifica que parte del sistema falla ya sea un hardware o un software.

- La duración de los fallos puede ser permanente o continuar indefinidamente en el tiempo.
- La extensión del fallo sólo afecta a un punto localizado o a la globalidad del hardware, software o de ambos.
- Los fallos pueden ser determinados si su fallo no cambia en el tiempo.

Redundancia

La redundancia es una de las técnicas frecuentemente más utilizadas para combatir los fallos. Consiste en integrar un hardware adicional con el fin de detectar fallos o conseguir tolerancia en los mismos y la redundancia de software consiste en integrar líneas de código adicionales para evitar errores.

La redundancia de software implica redundancia temporal, salvo si se emplea un procesador suplementario para ejecutar instrucciones existirá redundancia de hardware.

FUNDAMENTACIÓN SOCIAL

El proyecto de investigación a desarrollar cumple con los altos índices de seguridad de la información para garantizar la privacidad de los datos en la descentralización de la comunicaciones P2P con la implementación del protocolo OpenDHT que proporcionara confiabilidad y fiabilidad a los usuarios que pertenecen a una organización.

¿Qué impacto social tendrá la implementación del proyecto?

El proyecto de implementación del protocolo OpenDHT garantizará la seguridad de las comunicaciones P2P y que los activos de las empresas estén con cifrado robusto evitando el acceso de usuarios maliciosos, a la información de carácter sensible.

¿Cuál sería la solución que proporciona el protocolo de seguridad OpenDHT para resolver la problemática actual?

La implementación del protocolo OpenDHT resolverá la problemática de la falta de privacidad de los datos que transmiten los usuarios en comunicaciones P2P, cifrando o aplicando una técnica de encriptación robusta para garantizar la confidencialidad de la información.

¿Qué impacto tendrá en la comunidad?

La comunidad se beneficiará debido a que sus comunicaciones o la información de los usuarios estarán altamente seguras creando una dificultad a los atacantes maliciosos de tener acceso a la privacidad de los datos.

FUNDAMENTACIÓN LEGAL

CODIGO ORGANICO INTEGRAL PENAL

SECCIÓN TERCERA del COIP Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal

funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

LEY ORGANICA DE TELECOMUNICACIONES

INTERCONEXION Y ACCESO

CAPITULO I

Disposiciones comunes Art. 66.- Principios. La interconexión y el acceso. Deberán realizarse de conformidad con principios de igualdad, no-discriminación, neutralidad, buena fe, transparencia, publicidad y sobre la base de costos.

Art. 67.- Interconexión. A los efectos de esta Ley, se entiende por interconexión a la conexión o unión de dos o más redes públicas de telecomunicaciones, a través de medios físicos o radioeléctricos, mediante equipos o instalaciones que proveen líneas o enlaces de telecomunicaciones para el intercambio, tránsito o terminación de tráfico entre dos prestadores de servicios de telecomunicaciones, que permiten

comunicaciones entre usuarios de distintos prestadores de forma continua o discreta.

Art. 68.- Acceso. A los efectos de esta Ley, se entiende por acceso, a la puesta a disposición de otro prestador, en condiciones definidas, no discriminatorias y transparentes, de recursos de red o servicios con fines de prestación de servicios de telecomunicaciones, incluyendo cuando se utilicen para servicios de radiodifusión, sujetos a la normativa que emita la Agencia de Regulación y Control de las Telecomunicaciones, la misma que podría incluir entre otros los siguientes aspectos: el acceso a elementos y recursos de redes, así como a otros recursos y sistemas necesarios; las interfaces técnicas, protocolos u otras tecnologías que sean indispensables para la interoperabilidad de los servicios o redes.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

TÍTULO I
DE LOS MENSAJES DE DATOS Capítulo I PRINCIPIOS GENERALES

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.
El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

CAPÍTULO III
DE LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

DISPOSICIONES GENERALES
Novena.- Glosario de Términos.- Para efectos de esta Ley, los siguientes términos serán entendidos conforme se definen en este artículo:

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.
Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley.

Hipótesis

¿Usted cree que con la implementación del protocolo OpenDHT sus comunicaciones P2P estarán cifradas?

Sí, porque el protocolo obtiene una técnica de cifrado con un alto índice de seguridad a diferencia de otros protocolos donde los usuarios podrán enviar información a través de la red con la máxima protección de los datos.

¿El protocolo OpenDHT garantizará la confidencialidad, integridad y disponibilidad de la información?

El protocolo OpenDHT nos proporciona una técnica de seguridad avanzada en nuestros sistemas de comunicación P2P donde la confidencialidad, la integridad y disponibilidad de los datos estarán presentes, ya que con esto a los atacantes se les hará dificultoso poder tener el acceso a los activos de las organizaciones.

¿El protocolo OpenDHT le proporcionará la fiabilidad y confiabilidad en las comunicaciones P2P al transmitir los datos?

El protocolo OpenDHT es uno de los protocolos que garantiza la fiabilidad y confiabilidad en los sistemas P2P debido a la técnica de cifrado que posee éste con un alto índice de seguridad.

Variables de la Investigación

Variable dependiente: "Análisis de las ventajas del uso del protocolo OpenDHT"

Variable independiente: "para la descentralización de comunicaciones P2P"

DEFINICIONES CONCEPTUALES

COMUNICACIONES O REDES P2P

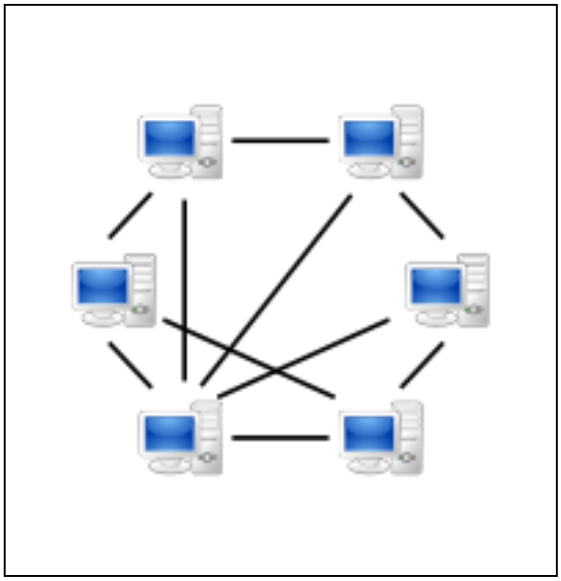
Son aquellas redes en las que no existen ni ordenadores cliente, ni ordenadores que hagan de servidor. Las redes P2P permiten el intercambio directo de información, en cualquier formato entre los ordenadores interconectados.

El hecho de que sirvan para compartir e intercambiar información de forma directa entre dos o más usuarios ha propiciado que hayan sido y estén siendo utilizadas para intercambiar archivos y demás contenido multimedia.[12]

Las redes peer-to-peer aprovechan, administran y optimizan el uso del Ancho de banda de los demás usuarios de la red por medio de la conectividad entre los

mismos, obteniendo más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.[12]

GRAFICO 4 REDES P2P



Fuente:https://www.ecured.cu/Red_Peer_to_Peer

Autor: Ecured

PROTOCOLO OPEN DHT

La búsqueda distribuida de Hash Table (DHT) es una técnica básica en redes estructuradas peer-to-peer (P2P). Su naturaleza descentralizada introduce vulnerabilidades de seguridad y privacidad para las aplicaciones construidas encima de ellos, así que se propuso diseñar un mecanismo de búsqueda que logre seguridad y anonimato, hasta ahora un problema abierto. Con el nuevo diseño de Octopus integrado con el protocolo OpenDHT, que utiliza mecanismos de identificación de atacantes para descubrir y eliminar nodos maliciosos, limitando severamente la capacidad de un adversario para llevar a cabo ataques activos y dividiendo las consultas de búsqueda por rutas anónimas separadas e introduciendo consultas ficticias para lograr altos niveles de anonimato.

Analizamos la seguridad de Octopus desarrollando un simulador basado en eventos para demostrar que los mecanismos de descubrimiento de atacantes pueden identificar rápidamente nodos malintencionados con baja tasa de error. Calculamos el anonimato de Octopus utilizando modelos probabilísticos y mostramos que Octopus puede lograr un anonimato casi óptimo. Evaluamos la eficiencia de Octopus en el laboratorio Planet y mostramos que Octopus tiene una latencia de búsqueda razonable y una carga de ancho de banda baja.[13]

CAPÍTULO III

METODOLOGÍA

DISEÑODE LA INVESTIGACIÓN

Modalidad dela investigación

El desarrollo científico e investigativo implica el uso de métodos que posibilitan el acopio de información o datos probados, acreditados e irrefutables, que para este caso investigativo se define con el siguiente modelo de porcentaje:

10%:Bibliografía.
10%:Campo “Entrevistas y Encuestas”.
80%:Creatividad “Propuesta”.

Tipo de investigación

Utilizaremos las siguientes modalidades de investigación:

- ✓ Aplicada
- ✓ Explicativo
- ✓ Cuantitativa
  - En otras palabras, la forma de razonar tiene relación con:
  - El cómo se entiende y comprende una realidad.
  - La significación que le otorga el sujeto a lo que estudia e investiga.
  - La dirección y el sentido que le adjudica a su objeto de estudio.
  - La intervención que hace el investigador.
  - Ampliar el conocimiento científico ya sea en la creación de teorías o replantear las ya existentes.
  - La resolución de problemas amplios y de validez general.
  - Crear conocimientos teóricos sobre los fenómenos sin ocuparse de su aplicación.

Según las referencias enmarcadas anteriormente la modalidad de Investigación a aplicarse será la siguiente:

Investigación Aplicada (IA).- También conocida como práctica o empírica, a diferencia de la Investigación Básica (IB) aplicamos los conocimientos que se adquieren de la investigación básica; se encuentra vinculada con la IB en tanto requiera de un enmarque teórico (resultados y avances), fundamentación y estado de las ideas que denoten coherencia en la recolección y sistematización de datos y del análisis e interpretación de la información.

En esta modalidad podemos encontrar la innovación técnica, artesanal e industrial, entre otras modalidades. Lo importante en la IA es saber y hacer, describir, explicar y aplicar, encontrar la verdad y lograr la eficiencia, "tener la verdad y accionar". El carácter utilitario es un criterio que orienta esta modalidad.

La IA tiene bases tanto teóricas como históricas, por esta razón la estructura de sus estudios cuenta con rigor metodológico y se constituye como un enlace entre la ciencia y la sociedad.

Tipos	**Conceptualización**	**Características**	**Finalidad**
Explicativo	Explicar lo que ocurre al alrededor, para ello estudia las relaciones que dan origen al problema o situación y sus aspectos, a través del uso de la teoría.	Plantea preguntas, diseña hipótesis o supuestos entornos a las causas y efectos de un problema.	Brinda a la sociedad y a la comunidad científica modelos teóricos, que se caractericen por ser explicativos, abstractos y universales. Elaborar predicciones con base en la ocurrencia de eventos.

Fuente: Trabajo de Investigación

Autores: Javier Briones-Héctor Hinojosa

Cuantitativa

El enfoque cuantitativo utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población.

Por lo común, en los estudios cuantitativos se establece una o varias hipótesis (suposiciones acerca de una realidad), se diseña un plan para someterlas a prueba, se miden los conceptos incluidos en la(s) hipótesis (variables) y se transforman las mediciones en valores numéricos (datos cuantificables), para analizarse posteriormente con técnicas estadísticas y extender los resultados a un universo más amplio, o para consolidar las creencias (formuladas en forma lógica en una teoría o un esquema teórico). Los estudios cuantitativos se asocian con los experimentos, las encuestas con preguntas cerradas o los estudios que emplean instrumentos de medición estandarizados. Además en la interpretación de los estudios hay una humildad que deja todo inconcluso e invita a seguir investigando y mejorar el conocimiento, poniendo a disposición de otros investigadores todos los métodos y los procedimientos.

M. A. Rothery y R. Grinnell, y Creswell (1997) describen estas investigaciones como estudios:

Patton (1980, 1990) define los datos cualitativos como descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones.

Explicativo

Consiste en encontrar respuestas a lo que sucede en el mundo, el sistema y la vida, por ejemplo explicar la naturaleza, las características; de un objeto, hecho o fenómeno que representa el problema que genera la pregunta.

POBLACIÓN

Es todo conjunto de elementos finito o infinito definido por una o más características de las que gozan todos los elementos que lo componen y sólo ellos.

En muestreo se entiende por población a la totalidad del universo que interesa considerar y que es necesario que este bien definido para que se sepa en todo momento que elementos lo componen.

En este caso se la realizará a personal especializado en sistemas distribuidos y entendidos del área.

MUESTRA

El muestreo es una herramienta de la investigación científica. Su función básica es determinar que parte de una realidad en estudio(población o universo) debe examinarseconlafinalidaddehacerinferenciassobredichapoblación.Elerror que se comete debido a hecho de que se obtienen conclusiones sobre cierta realidad a partir de la observación de sólo una parte de ella se denomina error de muestreo obtener una muestra adecuada significa lograr una versión simplificada de la población, que reproduzca de algún modo sus rasgos básicos.

PLANTEAMIENTO DE LA MUESTRA

Para ejecutar el cálculo de la muestra se toma en cuenta el volumen de la población y el margen de error. Luego de identificar que la población es finita, se aplica el proceso de hallazgo de la muestra con la utilización de la fórmula que se indica a continuación con los valores descritos para efectuar el reemplazo en el procedimiento y mostrar el resultado obtenido.

M= Tamaño de la población (450)

E= margen de error (6%)

n = Tamaño de la muestra

$$n = \frac{m}{e^2\,(m-1)+1}$$

SEGUNDO MÉTODO

$$n = \frac{450}{(0.06)^2(450-1)+1}$$

$$n = \frac{450}{0.0036(449)+1}$$

$$n = \frac{450}{1.6164+1}$$

$$n = \frac{450}{2.6164}$$

$$n = 171.99$$

$$n = 172\ personas\ a\ encustar.$$

Se determinó el tamaño de la muestra de 172 personas que laboran en empresas corporativas en el área de sistemas, las cuales se usaran para escoger los datos a analizar sobre los protocolos de seguridad para determinar los porcentajes e equivalencias de cada una las preguntas a realizar.

Muestra estratificada no proporcional

TABLA DE LA POBLACION Y LA MUESTRA

INVOLUCRADOS	POBLACION	MUESTRA	PORCENTAJE
Personal que laboran en el área de sistemas de las empresas corporativas	450	172	100%
TOTAL:	**450**	**172**	**100%**

Fuente: Trabajo de Investigación.
Elaboración: Javier Briones-Héctor Hinojosa.

TECNICAS E INSTRUMENTOS PARA LA RECOLECCION DE DATOS

Para la presente investigación en la recolección de datos se debe utilizar una serie de técnicas e instrumentos de análisis estadísticos para determinar la obtención de los datos que serán proporcionados por los especialistas en seguridad informática que laboran en el área de sistemas, a continuación se indicara las siguientes herramientas de recopilación de información.

Encuesta

Una encuesta es una técnica o método de recolección de datos en la cual procede a una persona interrogue a otra o a un grupo de individuos de manera verbal o por

medio de resolución de un cuestionario de preguntas con el fin de recopilar toda la información necesaria para una investigación especifica.[14]

Entrevista

Una entrevista es aquella cuando una persona hace el papel de asesor, esto consiste en plantear preguntas abiertas sobre un tema específico que van dirigida a las personas involucradas o especialistas que participan en dicha entrevista. Un los beneficios que proporciona la entrevista es la recolección de información importante y suficiente para establecer el nivel de factibilidad del tema que se está tratando en el transcurso de la audiencia.

RECOLECCIÓN DE LA INFORMACIÓN

Para llevar a cabo este proceso se elaboró una lista de preguntas que recalquen el tema a tratar “Análisis y uso de las ventajas del protocolo OpenDHT para la descentralización de comunicaciones P2P”.

Las encuestas realizadas fueron impresas en hojas formato A4 para ser entregadas al personal que labora en el área de sistemas en varias instituciones, este cuestionario está enfocado directamente a los especialistas en el área de seguridad informática, para manejar ideas, opiniones precisas y claras sobre cada ítem establecido en la investigación, esto ayuda a tener una mayor perspectiva para el levantamiento de información que se desea realizar y factibilidad de la misma.

Una vez finalizado el paso anterior, se procede a la tabulación de las incógnitas ejecutadas con la utilización de tablas valorativas donde se registraron todas las preguntas con su respectiva respuesta.

Durante el proceso se detalla la interpretación, las conclusiones y recomendaciones de los resultados obtenidos para como punto final dar realizar un resumen general y medir el nivel de factibilidad.

Los valores resultantes servirán como una guía a la aceptación del desarrollo de la propuesta por medio de la información conocida de los diferentes niveles de

personal, representa un estimado de acción para sostener la resolución del inconveniente planteado. Los datos muestreados están adjuntos dentro del presente documento, con su respectiva representación en tablas, con su análisis e interpretación para cada gráfico.

PROCESAMIENTO Y ANÁLISIS

El proceso y análisis surge luego de finalizar las encuestas a la muestra y se comienza a interpretar cada ítems. Se utilizó la herramienta Microsoft Excel, la cual permite desarrollar tablas dinámicas para la tabulación de datos por medio de la utilización de complementos como crear tablas y generar gráficos estadísticos, en este caso el diagrama de barra o el histograma de frecuencia, fue el seleccionado para la representación de salida.

Esto permite manejar una excelente distribución de la información para un adecuado análisis y compresión de la operación llevando así, a lograr la interpretación de datos concretos e ir obtenido los porcentajes generales para sustentar los argumentos y propuestas validos puntualizados en el presente documento.
Todo el proceso requiere seguir una serie de pasos sencillos para elaboración de cada opción mencionada en el texto:

1. Se plantearán un total de 5 preguntas.
2. El objetivo por el cual se formuló las preguntas; consultar las opiniones.
3. Elaborar una tabla con la frecuencia donde se indicara el nivel alto de los resultados obtenidos.
4. Representar gráficamente los resultados de la encuesta.
5. Análisis e interpretación de la información por cada pregunta.
6. Un resumen de los resultados obtenidos.
7. Se presentan la validación de la hipótesis.
8. Finalmente se elabora el documento respectivo de todo el proceso realizado.

ANÁLISIS DE LOS DATOS RECOLECTADOS

A continuación, se visualizarán los datos de la encuesta, entre esto es el origen del análisis e interpretación de resultados en base a la aplicación previa de los instrumentos y herramientas de recolección para la información obtenida.

En el proceso, cada pregunta fue enfocada al personal de empresas que laboran en el área de sistemas mediante la selección de repuesta en forma opcional.

El formulario está compuesto por 5 preguntas basadas en el protocolo OpenDHT con el objetivo de recopilar la información necesaria para verificar la aceptabilidad del proyecto de investigación. El propósito de la operación se asentó en compilación de datos para certificar, respaldar y conservar los resultados claros, exactos y evidenciables para dar sustentación al proyecto.

TABULACIÓNDELA ENCUESTA

Pregunta#1

conoce usted algún protocolo de seguridad de los nombrados a continuación:

OPEN DHT	
APPLETALK	
CHORD	
TORNP2P	

TABULACIÓN DE PREGUNTA No. 1 de Encuesta

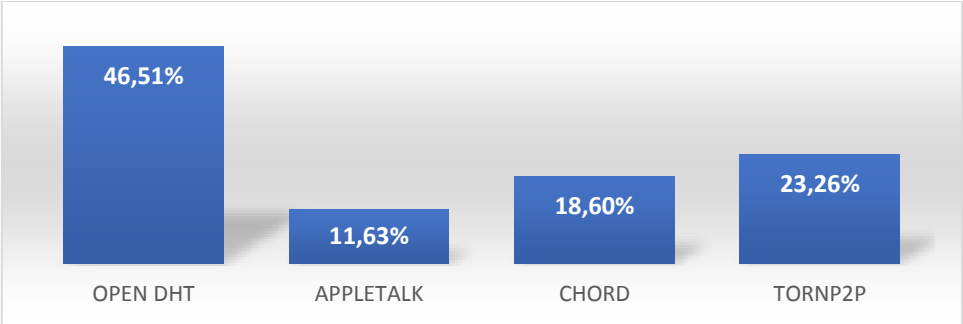
TABLA 3 PREGUNTA 1

PROTOCOLO	CANTIDAD	PORCENTAJE
OPEN DHT	80	46,51%
APPLETALK	20	11,63%
CHORD	32	18,60%
TORNP2P	40	23,26%
TOTAL	172	100%

Realizado por: Héctor Hinojosa – Javier Briones

GRAFICO NO. 5

TABULACIÓN DE PREGUNTA No. 1 de Encuesta



Realizado por: Héctor Hinojosa – Javier Briones

Fuente: Trabajo de Investigación

ANALISIS: Según los especialistas encuestados determinan y dan su aprobación como seguro el uso de los protocolos OPENDHT como herramientas de seguridad en sistemas informáticos

Pregunta#2

¿Usted confía en que el protocolo DHT que se usa para cifrado, además de gratuito es la solución óptima para las redes inteligentes?

SI ☐

NO ☐

DESCONOCE ☐

TABULACIÓN DE PREGUNTA No. 2 de Encuesta

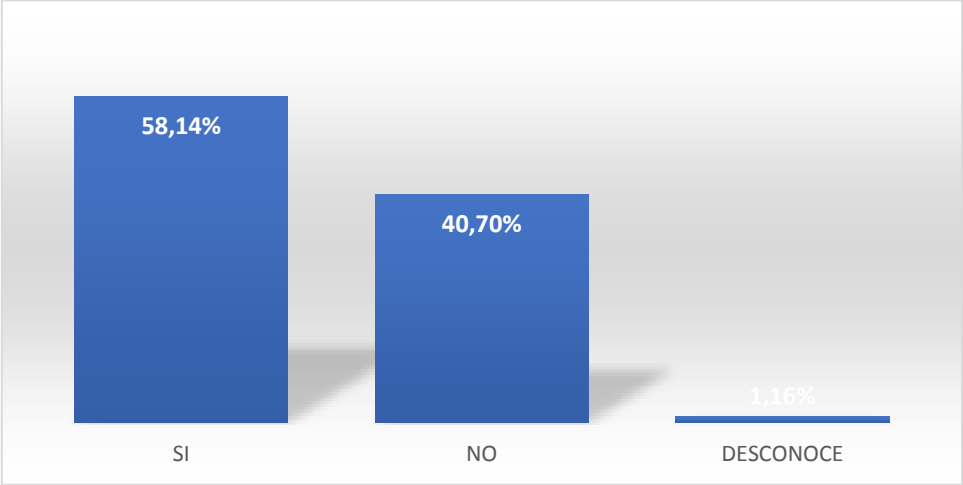
TABLA 4 PREGUNTA 2

DECISION	CANTIDAD	PORCENTAJE
SI	100	58,14%
NO	70	40,70%
DESCONOCE	2	1,16%
TOTAL	172	100%

Realizado por: Héctor Hinojosa – Javier Briones

GRAFICO NO. 6

TABULACIÓN DE PREGUNTA No. 2 de Encuesta



Realizado por: Héctor Hinojosa – Javier Briones

Fuente: Trabajo de Investigación

ANALISIS: Los datos de esta pregunta arrojan que es viable confiar en un protocolo OpenSource ya que el algoritmo tiende a actualizarse para hacer más robusto ante cualquier ataque.

Pregunta#3

¿El concepto de usar una tabla distribuida Hash, lo consideraría como solución viable ante la mejora de velocidad y seguridad en redes?

SI ☐

NO ☐

TABULACIÓN DE PREGUNTA No. 3 de Encuesta

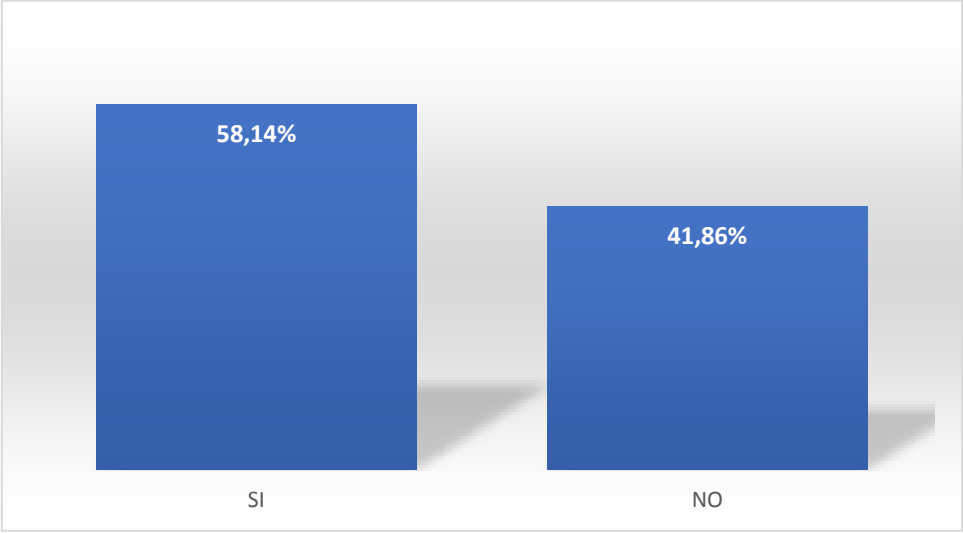
TABLA 5 PREGUNTA 3

DECISION	CANTIDAD	PORCENTAJE
SI	100	58,14%
NO	72	41,86%
TOTAL	172	100%

Realizado por: Héctor Hinojosa – Javier Briones

GRAFICO NO. 7

TABULACIÓN DE PREGUNTA No. 3 de Encuesta



Realizado por: Héctor Hinojosa – Javier Briones

Fuente: Trabajo de Investigación

ANALISIS: Así como la pregunta anterior indican que el uso de una tabla distribuida mejoraría notablemente la comunicación y seguridad de transmisión de esquemas operativos descentralizados dentro de cualquier empresa.

Pregunta#4

¿Cree usted que los sistemas descentralizados que usan P2P son pocos seguros o confiables, dentro de una arquitectura de red óptima?

SI ☐

NO ☐

TABULACIÓN DE PREGUNTA No. 4 de Encuesta

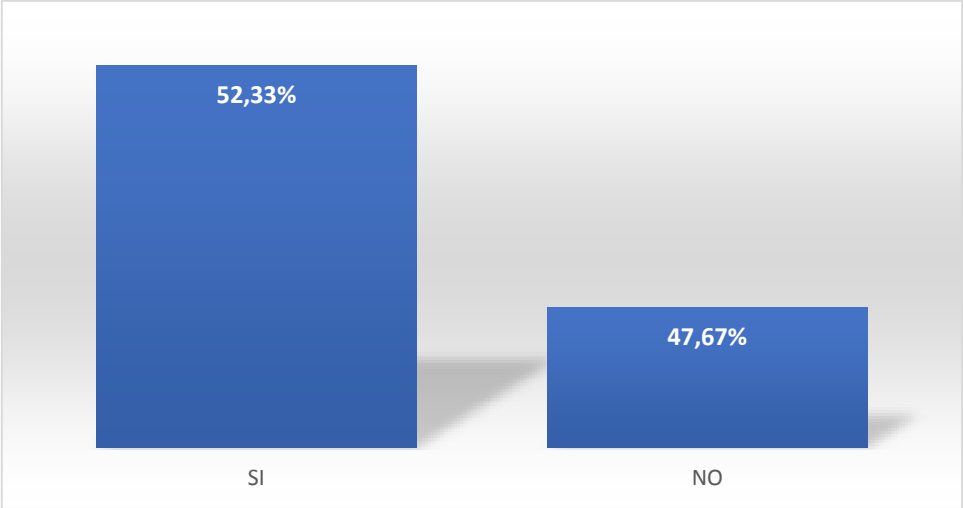
TABLA 6 PREGUNTA 4

DECISION	CANTIDAD	PORCENTAJE
SI	90	52,33%
NO	82	47,67%
TOTAL	172	100%

Realizado por: Héctor Hinojosa – Javier Briones

GRAFICO NO. 8

TABULACIÓN DE PREGUNTA No. 4 de Encuesta



Realizado por: Héctor Hinojosa – Javier Briones

Fuente: Trabajo de Investigación

ANALISIS: A diferencia de la pregunta anterior se nota un margen de afirmación muy corto debido a la duda que existe sobre los sistemas OpenSource sean más seguros que los sistemas propietarios.

Pregunta#5

¿Usted cree que la seguridad de sistemas descentralizados es óptima si se usan sistemas OpenSource?

SI ☐

NO ☐

TABULACIÓN DE PREGUNTA No. 5 de Encuesta

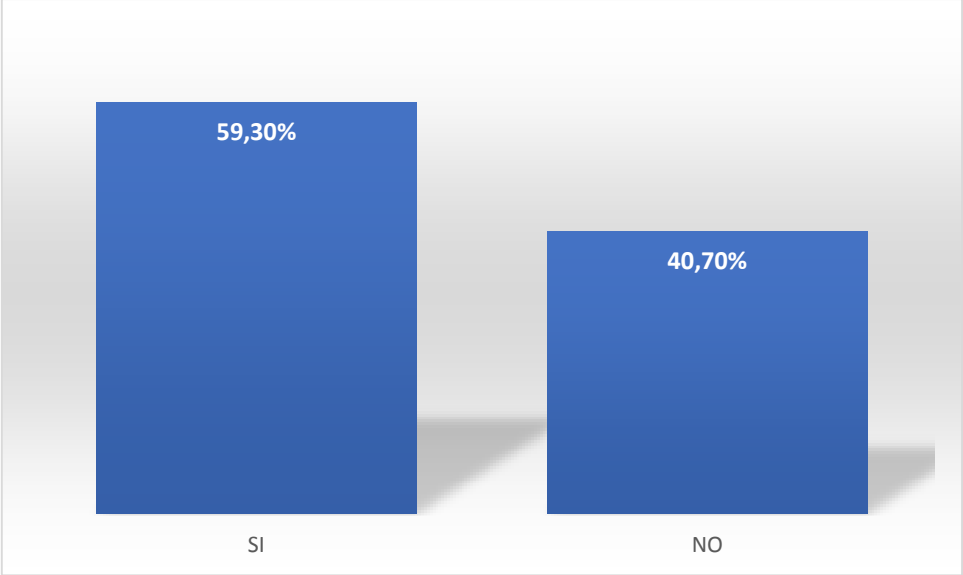
TABLA 7 PREGUNTA 5

DECISION	CANTIDAD	PORCENTAJE
SI	102	59,30%
NO	70	40,70%
TOTAL	172	100%

Realizado por: Héctor Hinojosa – Javier Briones

GRAFICO NO. 9

TABULACIÓN DE PREGUNTA No. 5 de Encuesta



Realizado por: Héctor Hinojosa – Javier Briones

Fuente: Trabajo de Investigación

ANALISIS: La afirmación se mantiene entre los encuestados, permitiendo asi seguir investigando en la problemática en mención..

Validación de la Hipótesis.

La propuesta del análisis de las ventajas del protocolo OpenDHT para la descentralización de las comunicaciones P2P, nos mostrara y permitirá analizar a las empresas que manejan o manipulan información de carácter confidencial e íntegro, buscando la factibilidad de que se implemente el protocolo de seguridad OpenDHT para cifrar o encriptar los datos sensibles de las organizaciones para así poder reducir el nivel de amenaza y riesgo de pérdida de información por parte de los atacantes maliciosos que intenten hacer daño a los activos de las empresas. Los resultados que se pueden conseguir con el estudio de dicha propuesta es contar con un sistema de encriptación mediante la integración de un canal cifrado donde se pueda transmitir la información de manera oculta por medio de la red. En el transcurso que duro la investigación del proyecto se anotaron requerimientos necesarios y a tener en consideración por intermedio del personal especialista en seguridad informática que laboran en distintas empresas sobre que sistemas informáticos carecen de un protocolo de seguridad robusto, buscando salvaguardar los datos y así poder obtener el nivel de aceptación de los involucrados.

Los valores proporcionados por medio de las encuestas al personal especialista en seguridad informática, dan sustentación al desarrollo del proyecto, dado que entre la muestra escogida existe gran cantidad del personal involucrado en el tema planteado, consiguiendo la transparencia y validez de los datos. Conocer los requerimientos, necesidades y nivel de aceptación ayuda a la contribución de una planificación más específica de estudio para aclarar dudas o corregir posibles errores inconsistentes que solo los usuarios operacionales pueden conocer y que podrían presentarse durante el levantamiento de información, o en tal caso durante la selección de protocolos de seguridad.

En la clasificación de consultados se meditaron varios puntos importantes para determinar un análisis de confianza, entre los cuales tenemos personal especialista en el área de seguridad. Con las limitaciones indicadas se puede llegar una desenlace más cercano para determinar la propuesta.

Al elaborar las encuestas, la mayoría del personal en mención estuvo de acuerdo con el desarrollo de la investigación, donde por medio del proyecto se pueden tomar las medidas adecuadas para el cifrado robusto de la información y dan el aceptamiento de la propuesta para una posible implementación del protocolo OpenDHT.

ANEXO

Pregunta#1

conoce usted algún protocolo de seguridad de los nombrados a continuación:

OPEN DHT

APPLETALK ☐

CHORD ☐

TORNP2P ☐

Pregunta#2

¿Usted confía en que protocolo rápido de encriptación y cifrado, además de gratuito es la solución óptima para las redes inteligentes?

SI ☐

NO ☐

Pregunta#3

¿El concepto de usar una tabla distribuida Hash, lo consideraría como solución viable ante la mejora de velocidad y seguridad en redes?

SI ☐

NO ☐

Pregunta#4

¿Cree usted que los sistemas descentralizados que usan P2P como pocos seguros o confiables, dentro de una arquitectura de red óptima?

SI ☐

NO ☐

Pregunta#5

¿Cree usted que los sistemas descentralizados que usan P2P como pocos seguros o confiables, dentro de una arquitectura de red óptima?

¿Usted cree que la seguridad de sistemas descentralizados es óptima si se usan sistemas OpenSource?

SI ☐

NO ☐

CAPÍTULO IV

PROPUESTA TECNOLÓGICA

Análisis de factibilidad

Dentro de las empresas que manejan información sensible no se cuenta con un área enfocada a la seguridad informática que permita salvaguardar la confidencialidad e integridad de los datos que se transmiten por medio de los sistemas informáticos y de la utilización de protocolos de seguridad con un nivel de escalabilidad alto para proteger los activos de las organizaciones, ya que pueden estar expuestos a posibles amenazas que dañen los activos físicos y lógicos de las corporaciones, para protegerse y evitar estos casos de ataques cibernéticos o amenazas que atenten a la confidencialidad de la información se deben tomar medidas de control para reducir o mitigar los riesgos que puedan ocurrir mediante un ataque realizado por un cracker , mismo que puede causar daños económicos a las compañías que tienen acceso autorizado a este tipo de información.[4]

Además se debe recordar que la seguridad informática es un área de suma importancia que nos ayuda a adoptar metodologías en la cual podemos identificar a que nivel de amenaza, peligro e impacto repercutido está expuesta la información transmitida por medio del sistema informático y la cual detalla que técnicas o medidas respectivas deben de tomar las organizaciones cuando se presente un incidente de seguridad.[4]

Como propuesta para el desarrollo del tema “Análisis y ventajas del uso del protocolo OpenDHT para la descentralización de comunicaciones P2P”, se ha planteado el levantamiento de información para validar el tipo de activos que obtienen las compañías y categorizarlos como importantes para la empresa. Con el protocolo OpenDHT se busca proteger los datos ante amenazas existentes que intenten dañar la información sensible de las organizaciones.

Entre las ventajas que obtiene este protocolo de seguridad en mención son las siguientes:

- Posee una capa de criptografía para la proporción de firmas digitales y técnicas de cifrado de información usando GNUTLS.
- Obtiene soporte para redes IPV4 e IPV6.
- Es un protocolo altamente escalable.
- OpenDHT reduce el costo y la dificultad de desarrollar aplicaciones
- OpenDHT construye una capa de cifrado en una red para verificar que los mensajes y firmas estén de manera íntegra.

Con estas ventajas que nos brinda el protocolo en mención podemos tomar todas las medidas de seguridad basadas en OpenDHT para tener una excelente encriptación en nuestra información.

Factibilidad Operacional

La factibilidad operacional consiste, en describir algunos componentes para determinar la viabilidad del proyecto:

Solución de la problemática planteada.

Como se ha indicado en capítulos anteriores la falta de un protocolo de seguridad robusto integrado en los sistemas informáticos de las organizaciones acarrea que existan fallos en la transmisión de los datos ya que por esto pueden vulnerar la confidencialidad e integridad de la información y los sistemas carecerían de fiabilidad y confiabilidad por parte de los usuarios que manejan información sensible en las empresas. Al comenzar el desarrollo de la misma se debe proveer soluciones de seguridad para evitar la intersección de los datos por parte de los delincuentes informáticos que pueden realizar afectaciones físicas como lógicas

en los activos. Esto hace que el proyecto sea requerido en la actualidad, como beneficio de la comunidad. Como se trata de un proyecto que involucra una dependencia importante a nivel educativo y laboral se necesita de operadores de la misma magnitud, cosa que en la actualidad se tiene y que da como factible operativamente el proyecto en todos los factores o puntos importantes.

Factibilidad Técnica

En esta fase se describen o se detallan todos los recursos técnicos que se necesitan para el análisis y ventajas del uso del protocolo OpenDHT en comunicaciones P2P y el por medio de esta investigación podemos definir las funcionalidades del mismo.

Los recursos de hardware y software requeridos para montar el protocolo son los siguientes:

- ✓ Sistema Operativo Linux
- ✓ Lenguaje de programación de JAVA para la configuración del protocolo
- ✓ Computadora portátil con procesado corel7.

Sistema Operativo Linux y herramientas de JAVA

Con este sistema operativo podremos detallar todas las ventajas, uso y funcionalidades del protocolo de seguridad en mención para la protección de las comunicaciones P2P.

Software: Las plataformas que se manejan en la tecnología de OpenDHT para el cifrado de redes P2P son las distribuciones de Linux con sus respectivos paquetes y las herramientas de entorno d JAVA

- ➢ Sistema Operativo (LINUX CENTOS)
- ➢ Lenguaje JAVA (NETBEANS)

Con estas herramientas se procese a investigar por medio de antecedentes de estudio las fases de pruebas del protocolo OpenDHT para verificar sus características que vienen implementadas en el mismo y además ver el tipo de cifrado que obtiene el protocolo de seguridad.

Factibilidad Legal

En esta fase no se vulneran las leyes vigentes en la república del Ecuador ya que el tema en mención es netamente investigativo donde se refiere a un análisis sobre el protocolo mencionado anteriormente y con esto se busca prevenir que el proyecto de investigación no se sienta afectado.

La factibilidad legal describe que los proyectos de investigación se vean afectados por parte de los desarrolladores que mediante pruebas informáticas pueden infringir las leyes vigentes en el Ecuador.

Factibilidad Económica

La viabilidad económica dependerá del valor que se invierta o el gasto que se realice en el momento de implementar el proyecto y verificar que los egresos generados no excedan el presupuesto financiero de la organización donde se requiera ejecutar el proyecto a largo plazo, evitando la paralización del mismo. El proyecto en desarrollo tiene una proyección a futuro, que cuenta con un margen de la cantidad que este dentro del presupuesto económico planteado para la elaboración del proyecto. Dentro de la propuesta se consideran varias herramientas de seguridad de código abierto, para una posible implementación del protocolo OpenDHT en las organizaciones que manejen información de carácter sensible en la cual no se maneja costos elevados, entre ellos se manejan software open source, haciéndolo factible económicamente.

Determinación de costos del proyecto

Es esencial determinar los gastos que las empresas puedan generar para la ejecución de la propuesta a largo plazo, a parte de otros costos que se detallan en términos anuales. Se recalca que el personal especialista en seguridad informática analiza la adquisición de una herramienta para la configuración y la ejecución del protocolo OpenDHT en comunicaciones P2P, en la cual tendrá una

capacitación previa sobre las especificaciones y puntos analizados sin ningún tipo de costo; no se incluyen licenciamiento de todo el software utilizado, dado que en su mayoría son Open Source que cumplan las necesidades actuales de las compañías.

Costos Fijos

Los costos fijos del proyecto se detallan en base a la realidad, y otros que surjan anualmente.

Costo de infraestructura y configuración del protocolo OpenDHT en comunicaciones P2P.

Levantamiento del servidor	$ 70.00
Migración de las aplicaciones al servidor levantado	$ 50.00
Configuración del protocolo de seguridad en el sistema	$ 25.00
Talento Humano	$ 20.00
Servicio de Internet	$ 20.00
Transporte	$ 15.00
TOTAL DE COSTOS FIJOS	$ 200.00

Etapas de la metodología del proyecto

Para el desarrollo del proyecto de investigación se eligió la metodología ITIL. Debido a su enfoque de gestión de los servicios informáticos para detallar las medidas respectivas para el desarrollo del proyecto.

La metodología ITIL en el proyecto cumple con las siguientes etapas en mención aquí indicaremos cada una de ellas.

Preparación del proyecto

Este es el primer paso para la aplicación de ITIL en el desarrollo del proyecto de OpenDHT, en donde se da a conocer al personal que labora en el área de sistemas en las compañías de la ciudad de Guayaquil, la consistencia del proyecto, las actividades a realizarse desde el inicio hasta el final de la propuesta, así como los objetivos que pretendemos alcanzar y ofrecerles información sobre el marco ITIL, de modo que se familiaricen y tengan algunos conocimientos sobre este.[15]

Es muy importante resaltar que este paso busca involucrar a todo el personal del área de seguridad informática para el desarrollo de la propuesta, debido a que son actores clave pues si ellos comprenden la importancia de aplicar las buenas prácticas ITIL y sus beneficios para el proyecto, entonces aportara con la información importante para la progresión de cada actividad o paso de implementación.[15]

Análisis de los procesos existentes

Aquí se va analizar, reconocer y evaluar los procesos que actualmente ejecuta las empresas en el sistema informático, con la finalidad de identificar los niveles de amenaza y riesgos que está expuesta la información donde los atacantes pueden vulnerar la confidencialidad, integridad y la disponibilidad de los datos causando daños económicos a las organizaciones.[15]

Generación de la estrategia

En este proceso se formularan las estrategias y acciones que se alinean a los objetivos del uso y ventajas del protocolo OpenDHT para la descentralización de comunicaciones P2P, las cuales a su vez se alinean a los objetivos específicos, con la finalidad de convertir la gestión del servicio, en un activo estratégico. Se reconocen las perspectivas sobre el área de sistemas de las empresas, se definen los usuarios, servicios y las prioridades de atención que debemos proteger para evitar los incidentes de seguridad en los activos de la organización.[15]

Planificación

Aquí se planificara el desarrollo de la propuesta a empresas que tengan implementado el departamento de TI dándoles a conocer el uso de este protocolo de seguridad en mención y las soluciones de seguridad altamente escalables que nos ofrece OpenDHT entre ellas la de brindar servicios de seguridad en entornos de calidad a los usuarios, para que su grado de satisfacción sea considerable y bastante aceptable, asegurando su preferencia por el protocolo mencionado anteriormente; además se formulan las

estrategias para el área y las acciones específicas basadas en ITIL, para llevarlas a cabo en la investigación desarrollada.[15]

También la metodología ITIL muestra las siguientes etapas o fases que debemos cumplir durante el desarrollo del proyecto.

- **DISEÑO:** Esta etapa se diseñara la estrategia de desarrollo del proyecto mencionado anteriormente cumpliendo todas sus características y requerimientos para ejecutar los procesos necesarios para el respectivo diseño de la propuesta, además se diseñará toda la documentación del mismo para la verificación de los resultados de investigación.

  En esta fase obtenemos lo siguientes procesos para el desarrollo del proyecto de investigación de OpenDHT: gestión del catálogo de servicio, gestión de los niveles de servicio, gestión de la disponibilidad, gestión de la capacidad, gestión de la continuidad de servicios de TI, gestión de la seguridad de la información y gestión de proveedores.
- **TRANSICION:** Se ocupa de toda la gestión y coordinación de los procesos y funciones del proyecto de investigación sobre el uso y ventajas del protocolo OpenDHT planificando una posible implementación del sistema de cifrado para llevar una excelente gestión de la seguridad de la información basada en esta metodología de estudio.
- **OPERACIÓN:** En esta última etapa se encarga de todas las actividades desarrolladas del proyecto de investigación para la gestión del servicio destinados a usuarios y empresas de carácter corporativo.

Grafico 5 Plan de Trabajo de ITIL

Fuente:http://www.dicomtech.com.pe/Consultoria_TI.html

Autor: Dicomtech

Detallamos la siguiente información para las metodologías ITIL a seguir tenemos:

Dueño de Producto: empresas que manejan información confidencial.
ITIL Master: Ing. Marlon Altamirano Di Luca
Equipo de trabajo ITIL: Javier Briones-Héctor Hinojosa.

El objetivo de la Estrategia de Servicio es el de incluir las TI (Tecnologías de la información y comunicación) en la Estrategia Empresarial de manera que se pueda calibrar los objetivos según nuestra infraestructura TI y adaptar cada uno a las necesidades y requerimientos del proyecto desarrollado. En esta metodología se diseñara un cronograma de actividades para la obtención de los resultados del proyecto en modo de investigación como parte principal y como eje en el Ciclo de Vida ITIL. Sin embargo, a pesar de este módulo de conocimiento, ITIL indica cómo comenzar a definir la Estrategia de Servicio, y por dónde comenzar a implantar estas mejoras que brinda el proyecto en mención a las infraestructuras de las organizaciones. La Estrategia de Servicio en ITIL se encamina hacia el mismo sentido que la estrategia empresarial, pero ahora incluyendo en ésta la componente TI. Integra pues a su análisis nuevos objetivos y la evolución futura de las TI en la Organización. El uso y ventajas del protocolo OpenDHT por medio de la metodología ITIL se busca alinear e integrar la tecnología con el Negocio para la gestión de salvaguardas hacia la confidencialidad e integridad de los datos y que los servicios tecnológicos que sean implementados estén integrados con el protocolo de seguridad en mención. Además que este mecanismo de seguridad se ejecute en los departamentos de TI y se diseñe para apoyar al negocio. La idea de este protocolo OpenDHT se trata de aportar a las organizaciones en satisfacer las necesidades de seguridad de la información que obtienen las empresas por la falta de sistemas de encriptación, planear para el futuro este tipo de proyecto sabiendo las necesidades de las compañías por cifrar sus activos lógicos y así se invierte para mejorar una infraestructura TI, o planificar el futuro de la empresa dependiendo de la capacidad actual en TI, y/o abrir nuevas líneas de negocio debido a que permite diferenciar del resto de empresas en las características que ofrece nuestra infraestructura TI. Con el fin de comenzar a integrar las TI en la estrategia se de tener en cuenta que uno de los principales defectos de toda organización (en todo el mundo) es que una vez tomada la decisión de comenzar a gestionarse y planificar su futuro, lo normal es que nunca se hayan definido

exactamente qué tipo de servicios relacionados con la TI ofrece la empresa y a quién y cómo dirigir los esfuerzos comerciales para ponerlos en el mercado.

Conclusiones de la metodología ITIL

ITIL es una de las metodologías que nos permite llevar a cabo toda la gestión del proyecto de uso y ventajas del protocolo OpenDHT para la descentralización de comunicaciones P2P de una manera investigativa o planificada para que en el futuro otro grupo de trabajo ejecute de un modo práctico el proyecto. También es importante conocer el tamaño real de la metodología ITIL, y considerar que se debe elegir una métrica o unidad de trabajo estandarizada para medir el esfuerzo de su implementación, esta unidad de trabajo podrían ser los servicios principales que se diseñan, implementan, operan y mejoran en el proyecto de adopción de ITIL.

TABLA 7 PRODUCT BACKBLOG

N°	HILOS
1	Revisión de anteproyecto
2	Entrega del anteproyecto corregido
3	Entrega de avances del capítulo 1
4	Entrega del capítulo 1 completo
5	Entrega de la corrección del capítulo 1
6	Reunión de coordinación del capítulo 2, 3 y 4
7	Entrega de avances del capítulo 2
8	Entrega del capítulo 2 completo
9	Entrega de avances del capítulo 3
10	Entrega del capítulo 3 completo
11	Entrega de avances del capítulo 4
12	Entrega del capítulo 4 completo

Fuente: Datos de la investigación.
Elaboración: Javier Briones-Héctor Hinojosa.

Entregables del proyecto

En esta fase por medio de la metodología ITIL se presentará la propuesta del uso ventajas del protocolo OpenDHT con sus respectivos costos y los resultados de investigación factible del protocolo en mención.

Anexos

Los anexos contendrán todas las posibles soluciones de seguridad a la confidencialidad de la información basado en el protocolo OpenDHT y se medirá la satisfacción del cliente para la posible ejecución del proyecto en los sistemas descentralizados de las comunicaciones P2P.

El objetivo de los resultados, mencionado previamente en el tema de OpenDHT desarrollado en el proyecto de titulación, es detallar las posibles soluciones de seguridad que nos brinda el protocolo en mención, medir y analizar los requerimientos del cliente, poder comprobar si existe un cumplimiento en los objetivos específicos.

Propuesta de Implementación del proyecto a largo plazo

Esta propuesta será elaborada en Microsoft Excel donde se detallara la planificación del proyecto, requerimientos del cliente, costos del proyecto, cronograma de actividades para el desarrollo del proyecto y los resultados del uso y ventajas del protocolo OpenDHT para la descentralización de comunicaciones P2P.

Criterios de validación de la propuesta

La validez del presente proyecto “Análisis y ventajas del uso del protocolo OpenDHT para la descentralización de comunicaciones P2P”, se da por medio de las soluciones que proporciona en la toma de decisiones para el área de seguridad informática para la salvaguardia de los activos de las empresas y de nuevas tecnologías de comunicaciones P2P integradas en las empresas.

Una vez finalizado el análisis de perspectiva o viabilidad con cada una de sus respectivas etapas, dando como resultado la factibilidad del mismo. Se verificara que lo expuesto dentro del documento desde la investigación realizada y recursos

detallados, se procese a culminar la investigación del proyecto para una futura implementación.

Criterios de aceptación del Producto o Servicio

Criterios de aceptación

TABLA 8 CRITERIOS DE ACEPTACION

Escenarios	Resultado esperado	Observación
Levantamiento de información de todos los activos de la organización.	Conteo de Activos	
Realización de encuesta dentro del establecimiento objeto de estudio	Se entrevistó al personal de la organización.	
Validación de Protocolo OpenDHT para la gestión del cifrado.	Análisis de sus ventajas, características y calidad	
Resultados Investigativos del Protocolo de Seguridad en mención	Validación de las funcionalidades del protocolo.	
Detalle de los servicios donde manejan información sensible	Categorización del tipo de información que se intenta proteger.	
Verificar resultados finales	Toma de decisiones	

Fuente: Datos de la investigación.
Elaboración: Javier Briones-Héctor Hinojosa

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Por medio del caso de estudio analizado, se comprobó que el sistema sigue funcionando, debido a que el protocolo OpenDHT brinda facilidades cuando se presenten fallos como el exceso de peticiones por parte de los usuarios y la comunicación entre nodos, ya que este protocolo OpenDHT facilita listas de enrutamiento de forma dinámica que permiten restaurar la comunicación de forma imperceptible para el usuario.

- Este protocolo de seguridad proporciona redundancia entre nodos, en los cuales, si llegase a existir un colapso en un enlace de la red los demás responden por el nodo inhabilitado proporcionando continuidad en la operación del sistema, debido a que los servicios se mantendrán conectados con enlaces auxiliares, garantizando la operatividad y robustez de los enlaces.

- El nivel de cifrado (SEGURIDAD) es compatible con todas las tablas HASH para el enrutamientos de contraseñas de usuarios debido a que las claves se actualizan en un periodo de tiempo determinado con un nuevo cifrado, gracias a que el algoritmo de OpenDHT garantiza la codificación de claves y usuarios en una nueva matriz hash.

- El protocolo OpenDHT almacena la información transmitida por medio de la red en contenedores de discos virtuales con la finalidad de salvaguardar la confidencialidad e integridad de los datos por que el protocolo de seguridad tiene conexión con servidores de Backup proveyendo una confiabilidad alta al sistema.

- El protocolo de seguridad garantiza la protección de los datos de carácter sensible mediante el uso de protocolos criptográficos los mismos que ayudan a reducir el nivel de amenaza a los que están expuestos las organizaciones, cumpliendo con los objetivos de los protocolos de encriptación robustos.

Recomendaciones

- Implementar un sistema tolerante a fallos para la conectividad de la red de forma continua, para reducir el riesgo de colapso del sistema por excesivas peticiones por parte de los usuarios al servidor de aplicaciones.

- Implementar un esquema de redundancia para la red tenga un enlace auxiliar y los servicios continúen ejecutándose constantemente y a su vez evitando las caídas de los mismos.

- Adaptar a los sistemas de tablas de algoritmos HASH integradas con el protocolo OpenDHT para el enrutamiento de contraseñas de forma segura para evitar el acceso a usuarios no autorizados.

- Validar e integrar todos los sistemas criptográficos con el protocolo OpenDHT para reducir el nivel de riesgo y amenaza hacia la confidencialidad, integridad y disponibilidad de los datos de gran importancia para que exista confiabilidad en el sistema donde los usuarios puedan tener acceso al mismo de una manera segura.

BIBLIOGRAFÍA

[1] S. M. R. Tam, *SpringerBriefs en Optimización er*. 2013.

[2] D. A. Tran, *Data Storage for Social A social aware approach*. 2012.

[3] H. Zhang, Y. Wen, H. Xie, and N. Yu, *Distributed Hash Table Theory , Platforms and Applications*. 2013.

[4] J. Martínez, J. Mejía, and M. Muñoz, “Análisis de la Seguridad en Internet de las Cosas : Una Revisión Sistemática de Literatura Security Analysis of the Internet of Things : A Systematic Literature Review,” 2016.

[5] D. Caragata, U. Tecnica, F. Santa, K. Tabia, U. Tecnica, and F. Santa, “Cryptanalysis of a chaos-based encryption algorithm for distributed systems,” pp. 31–36, 2013.

[6] M. N. Al-Ameen and M. Wright, “IPersea: Towards improving the Sybil-resilience of social DHT,” *J. Netw. Comput. Appl.*, vol. 71, pp. 1–10, 2016.

[7] J. M. B. Rocamora and J. R. I. Pedrasa, “Evaluation of hierarchical DHTs to mitigate churn effects in mobile networks,” *Comput. Commun.*, vol. 85, pp. 41–57, 2016.

[8] R. Gracia-Tinedo, P. García-López, and M. Sánchez-Artigas, “Sophia: A local trust system to secure key-based routing in non-deterministic DHTs,” *J. Parallel Distrib. Comput.*, vol. 72, no. 12, pp. 1696–1712, 2012.

[9] J. A. Restrepo, “Man in The Middle, Ataque y Detección,” 2012. .

[10] J. Xu, W. Liu, and K. Zeng, “Monitoring Multi-Hop Multi-Channel Wireless Networks: Online Sniffer Channel Assignment,” *2016 IEEE 41st Conf. Local Comput. Networks*, pp. 579–582, 2016.

[11] “6 sistemas tolerantes a fallos 6.1.,” 2012.

[12] ECURED, “REDES PEER TO PEER,” 2017. .

[13] Q. Wang and N. Borisov, “Octopus: A secure and anonymous DHT lookup,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 325–334, 2012.

[14] C. Negocio, “Encuesta,” *12/10/2015*. [Online]. Available: http://www.crecenegocios.com/que-es-una-encuesta/.

[15] A. Escuela, P. D. E. Ingenier, and D. E. Computaci, “ITIL V3 PARA LA GESTIÓN DE SERVICIOS DE TI DEL ÁREA DE SERVICE DESK DE LA FACULTAD DE INGENIERÍA Y ARQUITECTURA – USMP,” 2015.