



UNIVERSIDAD DE QUINTANA ROO  
DIVISIÓN DE CIENCIAS E INGENIERÍA

---

COMPUTACIÓN EN LA NIEBLA:  
ARQUITECTURA, APLICACIONES Y  
SEGURIDAD

---

TRABAJO MONOGRÁFICO  
PARA OBTENER EL GRADO DE

INGENIERO EN REDES.

PRESENTA

ANGEL ARNOLD ROLANDO BRITO VALLE.

SUPERVISORES

DR. JOSÉ ANTONIO LEÓN BORGES.

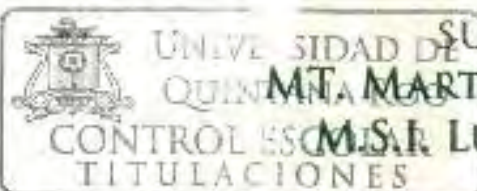
DR. HOMERO TORAL CRUZ.

DR. FREDDY IGNACIO CHAN PUC.

SUPERVISORES SUPLENTES

DR. MARTÍN ANTONIO SANTOS ROMERO.

DR. LUIS FERNANDO MIS RAMÍREZ.





**UNIVERSIDAD DE QUINTANA ROO**  
**DIVISIÓN DE CIENCIAS E INGENIERÍA**


TRABAJO MONOGRÁFICO TITULADO  
"COMPUTACIÓN EN LA NIEBLA: ARQUITECTURA, APLICACIONES Y SEGURIDAD"

ELABORADO POR  
**BRITO VALLE ANGEL ARNOLD ROLANDO**


BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y  
APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

**INGENIERO EN REDES**  
**COMITÉ SUPERVISOR**

**SUPERVISOR:**

  
DR. JOSÉ ANTONIO LEÓN BORGES


**SUPERVISOR:**

  
DR. HOMERO TORAL CRUZ


**SUPERVISOR:**

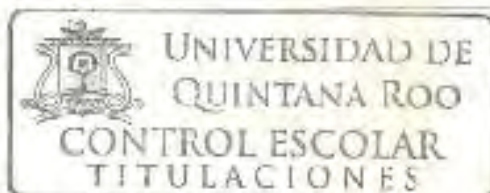
  
Dr. FREDDY IGNACIO CHAN PUC.

**SUPLENTE:**

  
M.T. MARTÍN ANTONIO SANTOS ROMERO.

**SUPLENTE:**

  
M.S.I. LUIS FERNANDO MIS RAMÍREZ.



## DEDICATORIAS.

A mis padres, que fueron la base fundamental de la persona que soy hoy en día, la educación comienza en casa, son un apoyo incondicional que sabes que podrás contar con ellos en todo momento y tienen la facultad de orientar en base a sus experiencias de esta vida que está llena de retos, superando expectativas.

A esta gran casa de estudios, la Universidad de Quintana Roo, que me formo con los más altos estándares de calidad y los maestros que te impulsan a seguir adelante creciendo como persona y profesionista con los mejores valores éticos.

## AGRADECIMIENTOS.

A esta gran casa de estudios, que me ha formado con los más altos estándares de calidad como profesional a lo largo de los años en la que se superaron obstáculos, tanto grandes como pequeños, así como lograr metas personales y formar las bases de lo que hoy en día soy como persona.

## RESUMEN.

La computación en la niebla (Fog Computing), es una extensión de lo que conocemos como computación en la nube (Cloud Computing), que extiende los servicios de la nube hasta el borde de la red para disminuir la latencia y la congestión de la red, es una tendencia de investigación relativamente reciente, aunque tanto cloud computing como fog computing ofrecen recursos y servicios similares, este último mencionado se caracteriza por una baja latencia con una extensión más amplia y nodos distribuidos geográficamente para soportar la movilidad y la interacción en tiempo real.

Cloud computing puede ser una alternativa eficiente para ser propietario, mantenimientos de recursos informáticos y aplicaciones para muchas organizaciones, particularmente organizaciones pequeñas y medianas debido al modelo de pago “*pay as you go*” por ejemplo bajo demanda, autoservicio, agrupación de recursos y elasticidad rápida.

Fog computing es un paradigma con capacidades limitadas como la informática, el almacenamiento y los servicios de red de manera distribuida entre diferentes dispositivos finales y la computación en la nube clásica. Proporciona una buena solución para aplicaciones sensibles de latencia.

En los últimos años, internet de las cosas (IoT) ha transformado los objetos de la vida cotidiana en dispositivos de comunicación. El número de dispositivos conectados será de 10 y 12 mil millones para 2021, lo que hace imposible que las tecnologías de red actuales admitan este enorme crecimiento. No se pensó que existiera tanta demanda de procesamiento y flujo de datos, quien imaginaria que se podría conectar desde un smartphone, hasta una ciudad inteligente (Smart City) en la red. Fog Computing ayuda a que la nube maneje la gran cantidad de datos que se generan diariamente desde el IoT. Permite una amplia gama de beneficios, que incluyen seguridad mejorada, ancho de banda y latencia reducidos. Estos beneficios hacen que la niebla sea un paradigma apropiado para muchos servicios de IoT en diversas aplicaciones, como vehículos conectados y redes inteligentes entre otros. Sin embargo, los dispositivos en “la niebla” obviamente enfrentan varias amenazas de seguridad, muy similares a las que enfrentan los centros de datos tradicionales, y que deben abordarse.



## CONTENIDO

<b>Dedicatorias.....</b>	<b>5</b>
<b>Agradecimientos.....</b>	<b>6</b>
<b>Resumen.....</b>	<b>7</b>
<b>Indice de ilustraciones.....</b>	<b>14</b>
<b>Índice de tablas.....</b>	<b>14</b>
<b>Indice de abrevaciones.....</b>	<b>15</b>
<b>Capitulo 1. Introducción.....</b>	<b>18</b>
<i>PROBLEMÁTICA ACTUAL.....</i>	<i>20</i>
1.1. COMPUTACIÓN EN LA NIEBLA.....	20
1.2. Características de la computación en la niebla.....	22
1.2.1 Ancho de banda.....	22
1.2.2. Soporte de movilidad.....	22
1.2.3. Baja latencia.....	23
1.2.4. Heterogeneidad en la naturaleza.....	23
1.2.5. Distribución geográfica y datos descentralizados.....	23
1.2.6. Seguridad de datos y protección de privacidad.....	23
1.2.7. Bajo consumo de energía.....	24
1.2.8. Interoperabilidad.....	24
1.2.9. Ventajas.....	24
1.2.10 Desventajas.....	25
1.3. Diseño de infraestructura.....	27
1.3.1. Infraestructura basada en Cloudlets.....	27
1.3.2. Infraestructura basada en virtualización.....	27
1.3.3. Planeación de la capacidad.....	28
<b>capitulo 2. arquitectura y taxonomía.....</b>	<b>29</b>
2.1. ARQUITECTURA.....	29
2.2. arquitectura jerárquica de la computación en niebla.....	29
2.2.1. Nivel terminal.....	29
2.2.2. Nivel de niebla.....	29

2.2.3. Nivel de nube .....	30
2.3. <i>Taxonomía</i> .....	31
.....	31
2.4. <i>Nodos de niebla</i> .....	32
2.4.1. Servidores .....	32
2.4.2. Dispositivos de red .....	32
2.4.3. Cloudlets .....	33
2.4.4. Estación base .....	33
2.4.5. Vehículos .....	33
2.5. <i>Colaboración nodal</i> .....	34
2.5.1. CLÚSTER .....	34
2.5.2. Peer to peer .....	34
2.5.3. Maestro esclavo .....	34
2.6. <i>Métricas para medir la calidad en el servicio</i> .....	35
2.6.1. Tiempo .....	35
2.6.2. Tiempo de computación .....	35
2.6.3. Tiempo de comunicación .....	35
2.6.4. La fecha límite (Deadline) .....	36
2.7. <i>Datos</i> .....	36
2.7.1. Tamaño de datos .....	36
2.7.2. Flujo de datos .....	36
2.8. <i>Costo</i> .....	37
2.8.1. Costo de red .....	37
2.8.2. Costo de despliegue .....	37
2.8.3. Costo de ejecución .....	37
2.9. <i>Contexto</i> .....	37
2.9.1. Usuario .....	38
2.9.2. Aplicación .....	38
2.10. <i>Consumo energético y huella de carbono</i> .....	38
2.11. <i>Objetivos de la computación en la niebla</i> .....	39
2.12. <i>Gestión de la latencia</i> .....	40
2.13. <i>Gestión del costo</i> .....	41
2.14. <i>Gestión de red</i> .....	41

2.14.1. Congestión de red .....	41
2.14.2. Virtualización .....	42
2.14.3. Conectividad.....	42
<b>2.15. Gestión de la computación.....</b>	<b>43</b>
2.15.1. Distribución de recursos.....	44
2.15.2. Asignación de carga de trabajo.....	44
2.15.3. Coordinación .....	44
<b>2.16. administración de aplicaciones .....</b>	<b>44</b>
2.16.1 plataforma de programación (Programming platform) .....	45
2.16.2. Escalamiento “ajuste” (Scaling). .....	45
2.16.3. técnicas de descarga (Offloading) .....	46
<b>2.17. Gestión de datos .....</b>	<b>46</b>
<b>2.18. Gestión de energía.....</b>	<b>46</b>
<b>2.19 SISTEMA DE RED APLICABLE .....</b>	<b>46</b>
<b>2.20. IoT .....</b>	<b>46</b>
<b>2.21. Mobile network / RAN.....</b>	<b>47</b>
<b>2.22. Red óptica pasiva de largo alcance / Comunicación de línea de alimentación (LRPON / PLC) .....</b>	<b>47</b>
2.22.1 La Red Óptica Pasiva de Largo Alcance (LRPON) .....	47
2.22.2 La comunicación por línea eléctrica (PLC) .....	48
<b>2.23. Red vehicular .....</b>	<b>48</b>
<b>2.24. Red de distribución de contenido (CDN).....</b>	<b>48</b>
<b>2.25. seguridad en la niebla. ....</b>	<b>48</b>
2.25.1. Autenticación .....	48
2.25.2. Cifrado .....	49
2.25.3. Privacidad.....	49
2.25.4. Ataque DoS .....	49
<b>capitulo 3. Aplicaciones .....</b>	<b>50</b>
3.1. Computación de niebla vehicular .....	50
3.2. Ciudades inteligentes.....	51
3.3. Autopistas inteligentes. ....	52



3.4. Telefonía 5G.....	52
3.4.1. Fog computing un requerimiento para las redes 5G.....	54
3.4.2. Arquitectura de red física .....	54
3.4.3. Capa del dispositivo .....	56
3.4.4. Capa de niebla .....	56
3.4.5. Capa de nube.....	57
3.4.6. Arquitectura de la aplicación .....	57
3.4.7. Componente del dispositivo .....	57
3.4.8. Componente de niebla .....	57
3.4.9. Componente de la nube .....	58
3.5. cuidado de la salud .....	59
3.6. realidad aumentada, interfaz de maquina de cerebro y juegos .....	60
3.7. Red de energía inteligente .....	61
3.8. Industria 4.0 y su relación .....	61
3.9. ambiente inteligente .....	62
<b>capitulo 4. Cloud, Edge, IoT and loE .....</b>	<b>63</b>
4.1. Computación en la nube .....	63
4.2. Computación en la niebla vs computación en la nube.....	64
4.3. Comunicación entre la computación en la niebla y en la nube.....	64
4.4. Computación en el borde y computación en la niebla .....	65
4.5. Internet de las cosas y la computación en la niebla .....	67
4.6. Retos para la computación en la niebla.....	67
4.7. Niebla en IoT y Cloud of Things.....	68
4.8. Internet of everything.....	69
4.8.1. Personas .....	70
4.8.2. Cosas .....	70
4.8.3. Datos .....	71
4.8.4. Procesos .....	71
<b>Capitulo 5. seguridad.....</b>	<b>74</b>
5.1. Problemas abiertos .....	74
5.1.1. Hombre a la mitad .....	74

5.1.2. Distribución denegada del servicio .....	74
5.1.3. Tolerancia a errores .....	75
<b>5.2. Confianza .....</b>	<b>75</b>
5.2.1. Engaño de colusión .....	75
5.2.2. Seguridad y protección de la privacidad .....	76
5.2.3. Confianza en Middleware y Specimen .....	77
5.2.4. Confianza basada en el área .....	78
<b>5.3. Penetración .....</b>	<b>79</b>
5.3.1. Nodos maliCIOUSos y sus penetraciones.....	79
5.3.2. Penetración MitM .....	80
<b>5.4. Control de acceso .....</b>	<b>81</b>
5.4.1. cifrado de calidad .....	81
5.4.2 Perfil de comportamiento .....	82
<b>5.5. Comunicación segura.....</b>	<b>83</b>
<b>5.6. Protección de la privacidad .....</b>	<b>83</b>
5.6.1. Área de protección de la privacidad.....	83
5.6.2. Otra protección de privacidad .....	84
<b>5.7. Otros.....</b>	<b>85</b>
<b>capitulo 6. modelado y Simulación Fog computing .....</b>	<b>86</b>
6.1. IFogSim .....	86
6.3. Computación de niebla y borde: desafíos de modelado y simulación.....	87
6.3.1. Modelado de nivel de aplicación .....	88
6.4. Infraestructura y modelado a nivel de red.....	89
6.5. Movilidad .....	90
6.6. ADMINISTRACION DE RECURSOS.....	91
6.7. ESCALABILIDAD .....	94
6.8. Estudio acerca herramientas de modelado fog and edge .....	96
<b>capitulo 7. Desafíos y direcciones futuras de investigación.....</b>	<b>104</b>
7.1. Sistema de niebla SLA.....	104
7.2. Diseño de sistema de niebla multiobjetivo.....	104

7.3. Diseño de sistema de niebla con reconocimiento de ancho de banda.....	104
7.4. Diseño escalable de esquemas de niebla .....	105
7.5. Computación de niebla móvil.....	105
7.6. Monitoreo de recursos de niebla.....	106
7.7. Computación de niebla verde .....	106
7.8. Soporte SDN para niebla .....	107
7.9. Soporte de usuarios de alta velocidad.....	107
7.10. Seguridad del nodo de niebla .....	108
7.11. Selección del sitio del nodo de niebla.....	108
7.12. Diseño de sistema de niebla resistente .....	109
7.13. Federación de niebla.....	110
7.14. Computación de niebla P2P.....	110
7.15. Confianza y autenticación en sistemas de niebla heterogéneos.....	111
7.16. Descarga segura de niebla .....	111
7.17. Paas para la computación de niebla.....	111
7.18. Estandarización de la computación en niebla.....	112
7.19. Tecnologías de hardware para niebla.....	112
<b>CONCLUSIONES .....</b>	<b>124</b>
<b>Referencias .....</b>	<b>125</b>

## INDICE DE ILUSTRACIONES.

ILUSTRACIÓN 1 FOG & CLOUD COMPUTING .....	21
ILUSTRACIÓN 2 FUENTE GOOGLE ANCHO DE BANDA.....	22
ILUSTRACIÓN 3 ESTRUCTURA JERÁRQUICA .....	26
ILUSTRACIÓN 4. TAXONOMÍA FOG COMPUTING.....	31
ILUSTRACIÓN 5.- VEHÍCULOS COMO NODOS DE NIEBLA.....	33
ILUSTRACIÓN 6 SEGURIDAD EN LA NIEBLA .....	39
ILUSTRACIÓN 7 GESTIÓN DE RECURSOS .....	40
ILUSTRACIÓN 8 CONECTIVIDAD .....	43
ILUSTRACIÓN 9.- FOG MANAGMENT.....	43
ILUSTRACIÓN 10 SMART CITY .....	51
ILUSTRACIÓN 11 FOG MOBILE NODES.....	53
ILUSTRACIÓN 12.- ARQUITECTURA DE RED 5G .....	55
ILUSTRACIÓN 13.- ARQUITECTURA DE APLICACIÓN .....	59
ILUSTRACIÓN 14.- INDUSTRIA 4.0.....	62
ILUSTRACIÓN 15 CARACTERÍSTICAS DEL CLOUD COMPUTING.....	63
ILUSTRACIÓN 16.- PERSONAS, COSAS, DATOS Y PROCESOS DE IOE.....	72
ILUSTRACIÓN 17 IFogSIM FUENTE GOOGLE .....	87

## ÍNDICE DE TABLAS.

TABLA 1.- COMPARACIÓN ENTRE DIFERENTES SISTEMAS DE SALUD BASADOS EN FOG.....	59
TABLA 2.- OBJETIVOS COMPUTACION EN LA NIEBLA Y COMPUTACIÓN DE NUBE .....	65
TABLA 3 COMPUTACIÓN EN LA NIEBLA VS COMPUTACIÓN EN EL BORDE .....	66
TABLA 4 RETOS PARA LA COMPUTACIÓN EN LA NIEBLA .....	67
TABLA 5.- HERRAMIENTAS DE SIMULADOR NIEBLA Y BORDE: ESTUDIO COMPARATIVO.....	102
TABLA 6.- DESAFÍOS Y FUTURAS DIRECCIONES DE INVESTIGACIÓN.....	123

## INDICE DE ABREVIACIONES.

ABE	ATTRIBUTE-BASED ENCRYPTION
AC	ALTERNATING CURRENT
AR	AUGMENTED REALITY
BS	BASE STATION
CAPEX	CAPITAL EXPENSES
CDN	CONTENT DISTRIBUTION NETWORK
CEP	COMPLEX EVENT PROCESSING
CP-ABE	CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION
CPS	CYBER-PHYSICAL SYSTEMS
CPU	CENTRAL PROCESSING UNIT
CRAN	CLOUD RADIO ACCESS NETWORK
D2D	DEVICE-TO-DEVICE
DES	SIMULACIÓN DE EVENTOS DISCRETOS
DNS	DOMAIN NAME SERVICE
DOS	DENIAL OF SERVICE
ETSI	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
FIWI	FIBER-WIRELESS
FPGA	FIELD-PROGRAMMING GATE ARRAY
F-RAN	FOG RADIO ACCESS NETWORK
HCRANS	HETEROGENEOUS CLOUD RADIO ACCESS NETWORKS
IOE	INTERNET OF EVERYTHING
IOT	INTERNET OF THINGS
LE	LOW ENERGY
LRPON	LONG-REACH OPTICAL NETWORK
LTE	LONG TERM EVOLUTION
M2M	MACHINE-TO-MACHINE

M2P	MACHINE TO PEOPLE
MACC	MOBILE AD HOC CLOUD COMPUTING
MCC	MOBILE CLOUD COMPUTING
MEC	MULTI-ACCESS EDGE COMPUTING
MEFC	MOBILE EDGE FOG COMPUTING
NAT	NETWORK ADDRESS TRANSLATION
NFV	NETWORK FUNCTION VIRTUALIZATION
NOMA	NONORTHOGONAL MULTIPLE ACCESS
NPS	NET PROMOTER SCORE
OPEX	OPERATING EXPENSES
P2P	PEER TO PEER
P2P	PEOPLE-TO-PEOPLE
PDES	PARALLEL DISCRETE EVENT SIMULATION
PLC	POWER LINE COMMUNICATION
PSS	PUBLIC SYSTEM SUBSCRIPTION
QOE	QUALITY OF EXPERIENCE
QOS	QUALITY OVER SERVICE
RAN	RADIO ACCESS NETWORK
RRHS	REMOTE RADIO HEADS
RSU	ROAD SITE UNIT
SC	SUPERPOSITION CODING
SCADA	SUPERVISORYCONTROLANDDATAACQUISITION
SDN	SOFTWARE DEFINE NETWORK
SE	SPECTRAL EFFICIENCY
SIC	SUCCESSIVE INTERFERENCE CANCELATION
SLA	SERVICE LEVEL AGREEMENT
SLO	SERVICE LEVEL OBJECT
TPP	TRUSTED THIRD PARTY
VANET	VEHICULAR AD HOC NETWORK
VCDN	VIRTUAL CONTENT DISTRIBUTION NETWORK
VM	VIRTUAL MACHINE

VNF	VIRTUAL NETWORK FUNCTIONS
VPN	VIRTUAL PRIVATE NETWORK
WLAN	WIRELESS LOCAL AREA NETWORK
WSN	WIRELESS SENSOR NETWORKS



## CAPITULO 1. INTRODUCCIÓN

Durante los últimos años hemos vivido una revolución en la forma como las personas se comunican, interactúan, trabajan, etc. Esta revolución ha sido causada por dos tecnologías principalmente: los teléfonos inteligentes (Smartphone) y la computación en la nube (Cloud Computing). Esta arquitectura de dos capas, compuesta por los dispositivos finales y el entorno de la nube, ha permitido un desarrollo sin precedentes en las redes de comunicación [1].

Paralelamente, hemos sido testigos del desarrollo y la difusión de Internet de las cosas (Internet of Things - IoT). En entornos IoT, los múltiples dispositivos inteligentes interconectados que admiten tareas cotidianas generan una gran cantidad de datos, lo que generalmente se conoce como Big Data [1]. IoT ha transformado los objetos de la vida cotidiana en dispositivos de comunicación. Se pronostica que para 2020 habrá entre 50 y 100 mil millones de estos dispositivos conectados a Internet [2], lo que hace imposible que las tecnologías de red actuales admitan este enorme crecimiento. No se pensó que existiera tanta demanda de procesamiento y flujo de datos, ni se imaginó que se podría conectar desde un Smartphone, una ciudad inteligente (Smart City) en la red.

Para abordar este problema, se propuso el paradigma de la computación en la niebla (Fog Computing), que reside entre la nube (Cloud Computing) y los dispositivos IoT. En general, en el entorno Fog Computing, los dispositivos IoT están conectados a dispositivos Fog. Estos dispositivos Fog están ubicados cerca de los usuarios y son responsables del procesamiento y el almacenamiento intermedio. Uno de los desafíos clave para ejecutar aplicaciones IoT en un entorno Fog Computing, es la asignación de recursos y la programación de tareas [3].

Fog Computing ayuda a que la nube maneje la gran cantidad de datos que se generan diariamente desde los dispositivos IoT. Permite una amplia gama de beneficios, que incluyen seguridad mejorada, uso más eficiente del ancho de banda para disminuir congestiones en la red, una extensión más amplia y nodos distribuidos geográficamente para soportar la movilidad y la interacción en tiempo real y baja latencia. Estos beneficios hacen que la niebla sea un paradigma apropiado para muchos servicios IoT en diversas aplicaciones, tales como [4] [5]: ciudades inteligentes, telefonía 5G, cuidado de la salud y seguimiento de actividad, redes de energía inteligente, industria 4.0, redes inalámbricas

de sensores y actuadores, ambiente inteligente, computación en la niebla vehicular (vehículos conectados, semáforos inteligentes), IoT y sistemas ciberfísicos, tecnologías de almacenamiento, realidad aumentada, interfaz cerebro-máquina y juegos.

Mediante el presente trabajo monográfico, proporcionamos una descripción general de la computación de niebla, se revisan los principales conceptos y definiciones, sus paradigmas informáticos relacionados, incluidas sus similitudes y diferencias; se investigan numerosas arquitecturas propuestas y se describen a detalle los componentes de estas arquitecturas; se representan las principales aplicaciones y se aborda el tema de seguridad, debido a que los dispositivos en la niebla enfrentan diversas amenazas, muy similares a las que enfrentan los centros de datos tradicionales..

## PROBLEMÁTICA ACTUAL

En la actualidad a partir del surgimiento de la cuarta revolución industrial, tanto fabricas como las personas están más conectados a internet, esto mediante diferentes dispositivos tales como; celulares, computadoras, electrodomésticos, sensores y máquinas, que continuamente generan información, la cual es procesada y almacenada en la nube.

Para un mejor control y manejo de datos se desarrolló la tecnología fog computing, que consiste principalmente en pequeñas nubes para la acumulación de información de manera descentralizada, lo que mejora el control, seguridad y uso de datos.

### 1.1. COMPUTACIÓN EN LA NIEBLA

La computación en la niebla es un concepto que se desprende directamente de la computación en la nube, la cual podemos definir como un conjunto de servidores que desde una ubicación remota almacenan y procesan datos. Estos servidores de la nube pueden localizarse en lugares lejanos de los usuarios, lo que puede ser un problema para el tiempo y la velocidad en el servicio, por esta razón se creó el termino de niebla que hace relación al fenómeno natural en la siguiente analogía: si la nube está muy encima de nosotros y no la podemos tocar, la niebla es una nube más pequeña a nuestro alcance. Por esta razón con la neblina se busca tener una nube más cercana a los diversos aparatos y sensores generadores de datos, para de esta manera tener el procesamiento de información más cercano como se ilustra en la Ilustración 1.

Históricamente este paradigma ha tomado mayor relevancia con el surgimiento del internet de las cosas, por lo que muchos expertos han buscado una definición para este fenómeno, por ejemplo: la empresa CISCO define como: "Fog Computing es un arquitectura informática con un grupo de recursos que consiste en uno o más dispositivos (incluidos los dispositivos perimetrales) en el borde de la red y no respaldados exclusivamente por servicios en la nube, para proporcionar de forma colaborativa computación, almacenamiento y comunicación elásticas (y muchos otros servicios nuevos y tareas) en entornos aislados a una gran escala de clientes en proximidad" [1].

Con la computación en la niebla el procesamiento de datos es igual al de la nube, utilizando los mismos recursos: servidores, conmutadores, puertas de enlace,

enrutadores, decodificadores o puntos de acceso al igual su forma de trabajo eficiente en consumo de energía y latencia, lo cual resulta benéfico para la industria.

En este sentido el procesamiento de datos se vuelve más fácil y se permite que mayor número de aparatos electrónicos estén conectados a una misma red descentralizada más cerca del lugar donde se generan los datos.

Al tener el almacenamiento de datos a un nivel más bajo nos permite que la nube se vea menos saturada cada día, de esta manera solo se enviarán los datos que sean sumamente necesarios mientras que los que necesiten una mayor velocidad de procesamiento se quedarán en la neblina.

Con el crecimiento del internet de las cosas, la nube no será suficiente para la cantidad de datos que van a ser generados por los diferentes objetos conectados a internet por lo que es necesario el desarrollo de este recurso, por ejemplo: al tener una casa inteligente cada uno de los aparatos y sensores generan datos de manera continua, y la mayoría de ellos no son de suma importancia para el funcionamiento como la temperatura del horno mientras no hay nadie en la casa, por eso al tener la computación en la niebla este tipo de datos no será llevado a la nube y serán procesados de manera más rápido por los dispositivos que conforman esta estructura [1].

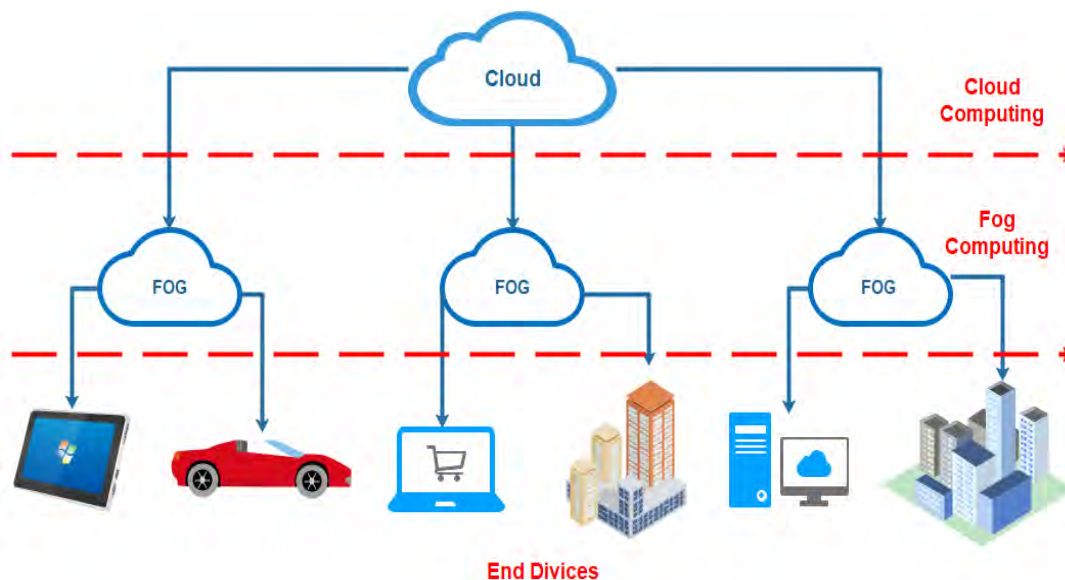


Ilustración 1 Fog & Cloud computing

## 1.2. CARACTERÍSTICAS DE LA COMPUTACIÓN EN LA NIEBLA

A continuación, se describen las principales características de la computación en la niebla, mostrando comparaciones con la nube.

### 1.2.1 ANCHO DE BANDA.

Para el ancho de banda en la computación en la nube, es necesario mencionar que los datos generados por los diferentes componentes electrónicos son almacenados en el borde de la red, esto es porque el sistema de niebla conectado a la nube selecciona y clasifica los datos, de manera que no toda la información es enviada a la nube y es procesada de manera local [1].

Por lo tanto, la computación de niebla podría reducir sustancialmente el volumen de transmisión de la red y en consecuencia de ancho de banda de salvamento. Además, los nodos de niebla, en el funcionamiento de ciertas aplicaciones, ejecutan toma de decisiones localmente, en lugar de cambiar el proceso a la nube y, en efecto, ahorrar ancho de banda importantemente [1].



*Ilustración 2 fuente Google ancho de banda*

### 1.2.2. SOPORTE DE MOVILIDAD

La computación en la niebla es flexible para los diferentes dispositivos, pueden ser estáticos o estar en movimiento, todo esto en apoyo al internet de las cosas, recientes

estudios relacionan la capacidad de relación de los teléfonos inteligentes con la computación en la niebla [2], esto al igual que diferentes dispositivos y sensores que se encuentran en el medio ambiente, ya sean estáticos como un semáforos o dinámicos como el sensor de un auto, esto contribuyendo a un servicio rápido y de calidad [2].

### 1.2.3. BAJA LATENCIA

Después de que los dispositivos generan datos, estos son almacenados y procesados en los nodos de niebla, lo que disminuye la interacción con la red y aumenta la velocidad en el servicio, lo que es benéfico para las aplicaciones que necesiten interacción en tiempo real [3].

### 1.2.4. HETEROGENEIDAD EN LA NATURALEZA

Los nodos de niebla pueden ser de virtuales o físicos, por lo que pueden ser utilizados en diferentes ambientes, comprendiendo gateways, enrutadores, estaciones base, puntos de acceso y servidores principalmente.

La computación en la niebla al ser compatible con el internet de las cosas, integra tecnologías de acceso inalámbrico como ZigBee, Wi-Fi, 3G, WLAN, 4G y también conexiones más rápidas que conectan con el centro de datos [4].

Las interfaces y los recursos de los nodos de niebla son sumamente contundentes y están diversificados en varias etapas de la jerarquía de diseño [5].

### 1.2.5. DISTRIBUCIÓN GEOGRÁFICA Y DATOS DESCENTRALIZADOS

La estructura de fog computing consta de muchos nodos distribuidos geográficamente en diversas localizaciones, las cuales permiten conocer la ubicación de los dispositivos, mientras que la información generada por los dispositivos se mantiene almacenada en los diferentes nodos comprendidos por la red, con la finalidad que la información esté siempre cerca de los usuarios [1].

### 1.2.6. SEGURIDAD DE DATOS Y PROTECCIÓN DE PRIVACIDAD

Como la computación en la niebla se encuentra cerca de los usuarios, así como sus recursos, la seguridad se debe de llevar al borde de la red, por lo que, para un mejor

manejo de datos, es necesario que el usuario haga uso de herramientas de protección a través de sistema de encriptación, lo que puede ser una desventaja para este tipo de sistema que se encuentra al alcance de cualquier usuario [1].

#### 1.2.7. BAJO CONSUMO DE ENERGÍA

Sabemos que en los centros de almacenamiento de datos gran parte de la energía se canaliza en el enfriamiento de los servidores, pero para la niebla este no es un problema, ya que su estructura de datos se distribuye de forma descentralizada y que no genera calor a gran escala, además de esto muchos de los nodos de niebla pueden ser alimentados con fuentes de energía limpia y pueden ser administrados para su consumo energético, por lo que puede ser una opción ecológica [1].

#### 1.2.8. INTEROPERABILIDAD

En la computación en la niebla los aparatos y los nodos son suministrados por diferentes compañías, distribuidos en diferentes lugares de manera descentralizada, estos pueden ser usados en diferentes escenarios, por lo que los proveedores pueden ofrecer una amplia gama de servicios [6].

Por ejemplo, al referirse a una carretera inteligente debe de existir operabilidad entre los diferentes automóviles, semáforos, sensores y cámaras. Necesitando un procesamiento y análisis rápido de los datos generados sin importar la fuente.

#### 1.2.9. VENTAJAS

Al ser una posible solución para mejorar el control de dispositivos en el internet de las cosas, se pueden esperar algunas ventajas con respecto a la computación en la nube, las cuales se describen a continuación:

- Al hacer una comparación con la nube se puede resaltar que la computación en la niebla es más rápida en tiempo real, ya que esta neblina se encuentra más cercana a los aparatos que la nube, teniendo una menor saturación por la menor cantidad de aparatos conectados.
- Una ventaja para el uso de este sistema es que los componentes usados para la edge y core networking pueden ser usados como nodos para la computación en



la niebla, y al usar este tipo de nodos, los diferentes aparatos electrónicos y sensores están más cerca de estos componentes, teniendo como consecuencia la latencia de las aplicaciones será minimizada significativamente.

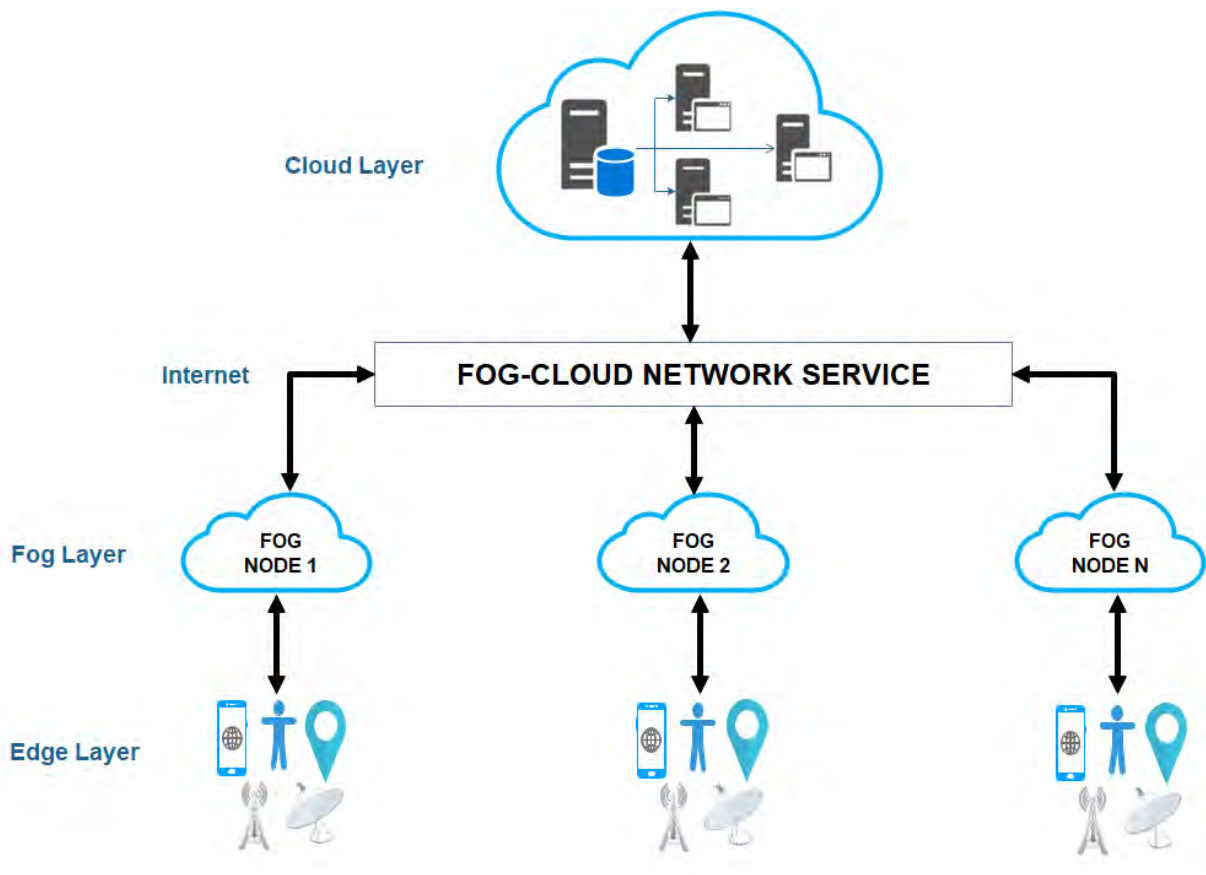
- Con los avances tecnológicos y el internet de las cosas, la computación en la niebla es compatible con estas nuevas tendencias, como la creación de redes para ciudades inteligentes.
- La computación en niebla facilita el conocimiento de la ubicación, Soporte de movilidad, interacciones en tiempo real, escalabilidad e interoperabilidad [7].
- Debido a que el control de la computación en la niebla no requiere de gran infraestructura como en la nube, este puede ser operado sin la necesidad de intervención de grandes compañías como en la nube por lo que es posible el uso de fog computing por empresas privadas o en servidores públicos
- El gran manejo de datos se verá optimizado al usar estas pequeñas neblinas, ya que no todos los datos serán enviados para su procesamiento, en cambio serán procesados y almacenados localmente
- Las empresas pueden tener su propia red para control interno, así como edificios, fábricas o hasta ciudades

#### 1.2.10 DESVENTAJAS

Aunque es una tecnología de vanguardia llega a tener algunas desventajas, principalmente respecto a la seguridad, aunque esta ha aumentado en los últimos años, también el robo de información crece de manera alarmante. A continuación se presentan algunas posibles desventajas de la implementación de esta nueva tecnología:

- La computación en la niebla puede verse afectada por algunos factores internos los que se ven reflejados en el uso de energía, el costo de uso y el flujo de datos entre otro.
- Ya que la infraestructura de esta red es diseñada sobre componentes tradicionales, es propensa a los ataques de seguridad, por lo que se debe de tomar medidas de precaución en esta área, aunque llegan a afectar la calidad en el servicio.

- Los controladores para proteger contra caídas y abusos, que generalmente se ubican en los bordes, son difíciles de proteger lo cual es un problema de vulnerabilidad.
- Un costo implicado para los diferentes hardware que implican la computación en la niebla, son los costos de mantenimiento ya que por la descentralización deben de llevarse por separado lo que implica un mayor costo en comparación a la nube. Estos lugares pueden procesar algunos datos de manera eficiente, para posteriormente ser desechados o compartidos a la nube. En este nivel es muy importante definir la ubicación de los nodos receptores para tener una buena calidad en el servicio, por lo que pueden ser instalados en zonas altamente concurridas como centros comerciales, zócalos, escuelas u hospitales entre otros.



*Ilustración 3 Estructura jerárquica*

### 1.3. DISEÑO DE INFRAESTRUCTURA

Actualmente la infraestructura para la computación en la niebla no ha sido muy estudiada ni definida, debido a la falta de protocolos estandarizados, aunque se han hecho algunas investigaciones de posibles infraestructuras como las que se hablan a continuación:

#### 1.3.1. INFRAESTRUCTURA BASADA EN CLOUDLETS

El objetivo del estudio es diseñar una red basada en redes ópticas pasivas multiplexadas por división de tiempo (TDM), para optimizar el costo de la infraestructura de la red y al mismo tiempo satisfacer las restricciones de latencia [12]. Dado que el costo de instalación de un cloudlet depende directamente del proveedor, ubicación y cantidad de recursos para los cloudlets, los proveedores de cloudlets deben tener en cuenta tanto el retraso de extremo a extremo de las solicitudes de los usuarios como el costo de la implementación [13].

#### 1.3.2. INFRAESTRUCTURA BASADA EN VIRTUALIZACIÓN

Para la infraestructura basa en virtualización es necesario el intercambio entre la computación y la comunicación, propone una arquitectura basada en F-RAN. La arquitectura basada en F-RAN consiste en un equipo de acceso de radio, nodos F-RAN que proporcionan los recursos de computación, dispositivos finales y un controlador F-RAN que está a cargo de recibir solicitudes de servicio y distribuir tareas a los nodos de niebla [14].

Algunos autores infieren que esta arquitectura puede satisfacer las demandas de aplicaciones de ultra baja latencia al confiar en las comunicaciones inalámbricas de frente y distribuir tareas de computación a múltiples nodos F-RAN cerca de los usuarios finales.

### 1.3.3. PLANEACIÓN DE LA CAPACIDAD

Muchos autores se han cuestionado dónde se deben de ubicar los centros de datos perimetrales y la capacidad de computo que debe asignarse para que esta infraestructura sea rentable y cumpla con los requisitos del cliente para el rendimiento y el ancho de banda. Existen diversos paradigmas acerca de la ubicación de centros de datos en la capa perimetral y en el borde para conocer el funcionamiento de los dispositivos y las aplicaciones.

## CAPITULO 2. ARQUITECTURA Y TAXONOMÍA

### 2.1. ARQUITECTURA

Fog computing, es una nueva plataforma que complementa la computación en la nube, traslada los trabajos convencionales en la nube, como la informática y los servicios al borde de la red. En el borde de la red, ofrece a los usuarios finales comunicación, almacenamiento, servicios, control y computación. La característica destacada de la computación de niebla es su descentralización. En su diseño y arquitectura, el cómputo de niebla está en desacuerdo con otros modelos tradicionales de cómputo [1].

### 2.2. ARQUITECTURA JERÁRQUICA DE LA COMPUTACIÓN EN NIEBLA.

Desde su aparición, para la computación en la niebla se han propuesto varios diseños. Pero la mayoría de ellos siempre ha dependido de una arquitectura de tres niveles. Como se mencionó anteriormente, la computación en la niebla desplaza los servicios en la nube al borde de la red. Lo antes mencionado se logra mediante la inyección de una capa de niebla entre la nube y los dispositivos finales. La estructura estratificada de la computación de niebla proviene de los siguientes tres niveles [1]: nivel terminal, nivel de niebla y nivel de nube.

#### 2.2.1. NIVEL TERMINAL

Este nivel es el más cercano al usuario final y al mundo físico. Abarca diferentes segmentos de IoT, como teléfonos celulares, sensores, tarjetas inteligentes, vehículos inteligentes, etc. En general, estos dispositivos se dispersan ampliamente y detectan y capturan la información característica de sucesos u objetos reales y luego transfieren la información detectada a los niveles anteriores, ya sea para guardar o procesar [1].

#### 2.2.2. NIVEL DE NIEBLA

Situado en el borde de la red, este nivel comprende muchos nodos de niebla, como conmutadores, enrutadores, puntos de acceso, puertas de enlace, servidores de niebla, estaciones base, etc. Entre la nube y los dispositivos finales, estos nodos de niebla están ampliamente dispersos, por ejemplo, ubicaciones tales como centros

comerciales, depósitos de autobuses, cafeterías, parques, calles, etc. Cualquiera que sea su posición, ya sea que se muevan en vehículos o estén fijos en un lugar, los nodos de niebla facilitan la conectividad con dispositivos finales para entregar servicios. Poseen el poder de transferir, cuantificar y guardar los datos recibidos a través de la detección. Es en el nivel de niebla donde tienen lugar las funciones sensibles a la latencia y el análisis en tiempo real. Además, a través de la red central IP, los nodos de niebla pueden vincularse con el centro de datos en la nube y trabajar conjuntamente e interactuar con la nube para adquirir fortalezas mejoradas para guardar y procesar [1].

### 2.2.3. NIVEL DE NUBE

Consiste principalmente en varios servidores de alta velocidad y nichos de almacenamiento, el nivel de computación en la nube es responsable de ofrecer diversos servicios de aplicaciones, como transporte inteligente, fábrica inteligente, hogar inteligente, oficina inteligente, etc. Este nivel posee capacidades gigantescas para el almacenamiento, guardar y computar, por lo tanto, ejecuta un amplio análisis de computación, almacena y guarda eternamente grandes cantidades de datos e información.

En este diseño, la conexión por cable o las tecnologías de acceso inalámbrico, como Wi-Fi, 3G, red de área local, 4G, Bluetooth, ZigBee y otras, ayudan a vincular cada elemento inteligente o dispositivo final con nodos de niebla. Las tecnologías de comunicación inalámbricas o cableadas también ayudan a los nodos de niebla a vincularse y comunicarse entre sí. Además de eso, a través de la red central IP, cada nodo de niebla permanece conectado con la nube.

Por lo tanto, esta arquitectura, en esencia, tiene la capacidad de ofrecer respaldo técnico a IoT, Internet móvil y CPS, para garantizar instalaciones de almacenamiento y procesamiento de datos competentes. Para controlar y monitorear los dispositivos y objetos que se encuentran en el mundo físico, CPS combina las competencias de comunicación, almacenamiento y computación. La computación en niebla puede mejorar la calidad del servicio y la competencia de CPS, especialmente en el escenario actual de proliferación de datos [1].

### 2.3. Taxonomía

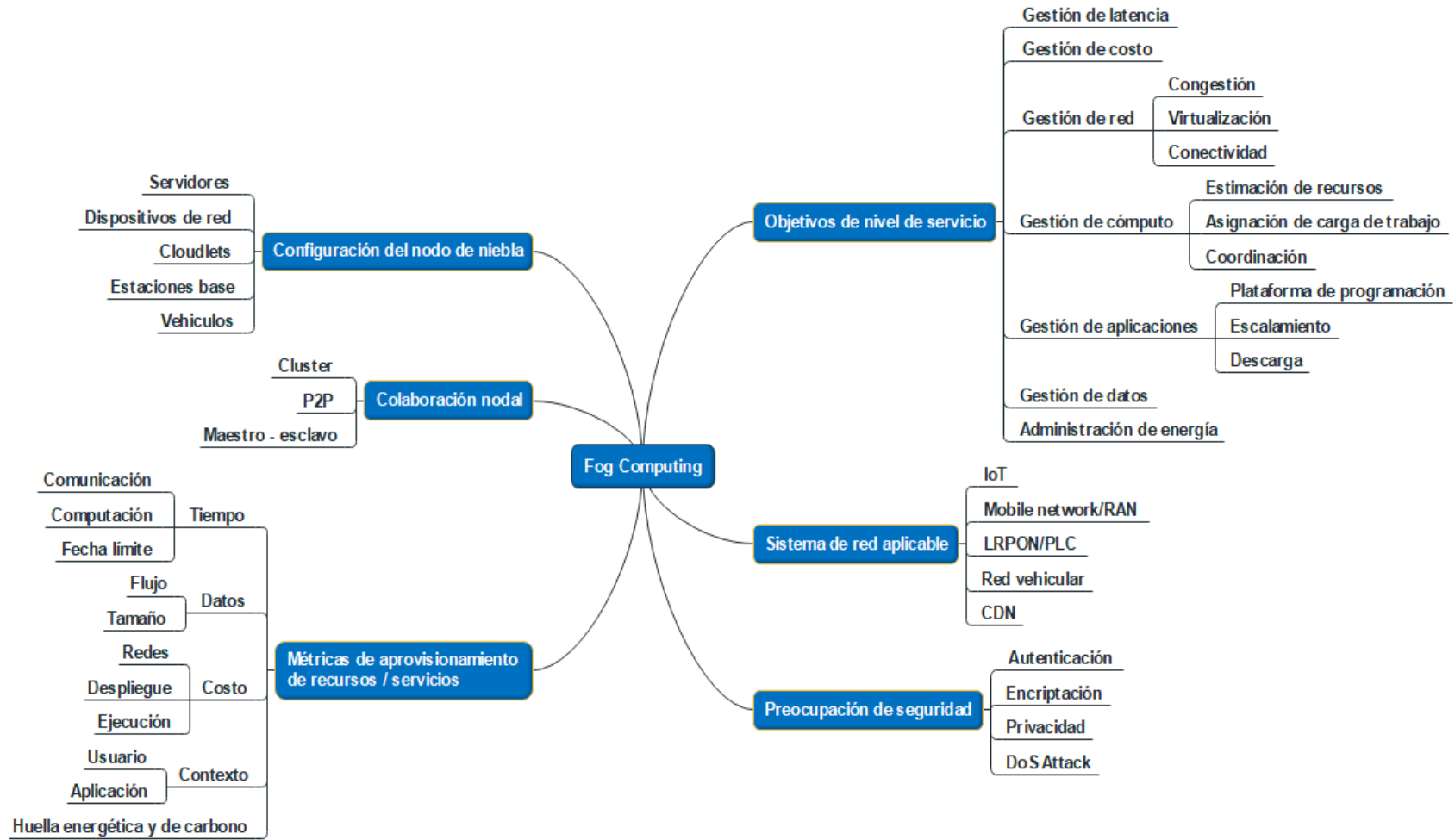


Ilustración 4. taxonomía fog computing



## 2.4. NODOS DE NIEBLA

Para el funcionamiento de la niebla es necesario contar con una red de diferentes dispositivos que controlen la información de forma descentralizada, por eso a continuación se explicarán los diferentes nodos de niebla.

### 2.4.1. SERVIDORES

Para que estos nodos tengan un amplio lugar de cobertura deben de ser instalados en lugares donde exista un gran número de usuarios tales como terminales de autobuses, centros comerciales, carreteras, parques, etc., por lo que en lugares concurridos son un lugar ideal, al igual que los servidores livianos de la nube, estos servidores de fog computing están virtualizados y equipados con instalaciones de almacenamiento, cómputo y redes. Hay muchos trabajos que han considerado a los servidores fog computing como el componente funcional principal de la computación de niebla, estos servidores llegan a ser muy pequeños y prácticos, contando con las mismas propiedades que los de la nube, están virtualizados y equipados con instalaciones de almacenamiento, cómputo y redes [15].

### 2.4.2. DISPOSITIVOS DE RED

Una ventaja de la computación en la niebla es que los dispositivos usados para la nube como enrutadores de puerta de enlace, decodificadores y conmutadores, entre otros, pueden formar parte de la arquitectura de la niebla. Los dispositivos como enrutadores de puerta de enlace, conmutadores, decodificadores, etc., además de sus actividades de red tradicionales (enrutamiento, reenvío de paquetes, conversiones de señales analógicas a digitales, etc.) pueden actuar como infraestructura potencial para la computación de niebla, la implementación distribuida de dispositivos de red ayuda a que la computación de niebla sea omnipresente, aunque la diversidad física de los dispositivos afecta significativamente el suministro de recursos y servicios [16], [17].

### 2.4.3. CLOUDLETS

Los cloudlets, son micro nubes ubicadas cerca de los dispositivos y sensores, las cuales se han diseñado para extender los servicios de la nube a los dispositivos móviles, estos pueden ser usados como nodos de niebla, en algunos casos, debido a restricciones estructurales, los cloudlets, incluso después de la implementación en el borde, actúan como componentes centralizados [18].

### 2.4.4. ESTACIÓN BASE

Actualmente las estaciones base son usadas en las redes móviles e inalámbricas para el procesamiento de datos y la comunicación eficiente, pero si a estas estaciones se equipan con ciertas capacidades de almacenamiento y computación pueden ser usadas en la computación en la niebla como nodos [19], [20].

### 2.4.5. VEHÍCULOS

Con motivo de la creación de carreteras y ciudades inteligentes, se podría implementar que los vehículos sean nodos de niebla, ya sea estando en movimiento o estacionados. Estos vehículos serían de gran importancia para crear un entorno altamente escalable, aunque este supuesto, puede ser afectado por problemas de privacidad.

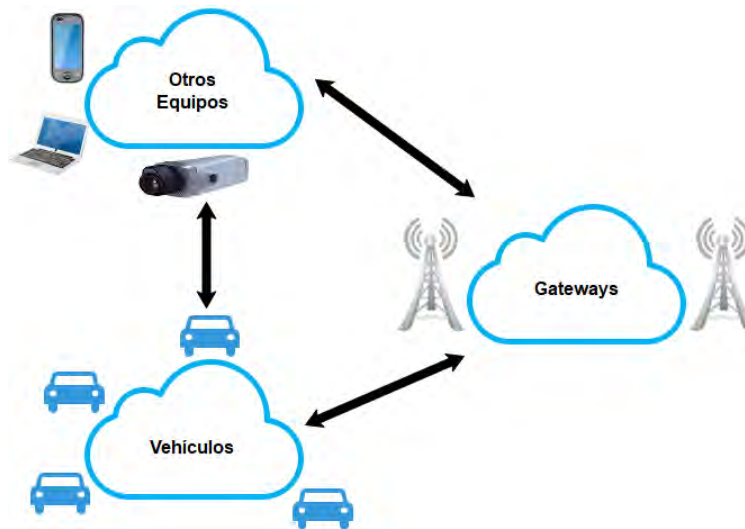


Ilustración 5.- Vehículos como nodos

## 2.5. COLABORACIÓN NODAL

### 2.5.1. CLÚSTER

Los nodos de niebla que residen en el borde pueden mantener un entorno de ejecución de colaboración formando un grupo entre ellos. Los grupos pueden formarse en función de la homogeneidad de los nodos de niebla o su ubicación. El equilibrio de carga computacional y el desarrollo del subsistema funcional también pueden recibir mayor prioridad al formar un clúster entre los nodos. La colaboración basada en clústeres es eficaz para explotar las capacidades de varios nodos de Fog simultáneamente. Sin embargo, los clústeres estáticos son difíciles de hacer escalables en tiempo de ejecución y la formación dinámica de los clústeres depende en gran medida de la carga existente y la disponibilidad de nodos de niebla. En ambos casos, la sobrecarga de redes juega un papel vital [2].

### 2.5.2. PEER TO PEER

En Fog computing Peer to Peer (P2P) la colaboración entre los nodos es muy común. La colaboración P2P se puede realizar tanto en orden jerárquico como plano. Además, según la proximidad, la colaboración P2P entre los nodos de Fog se puede clasificar como local (home), local, no local, etc. A través de la colaboración P2P no solo se procesa la salida de un nodo, aparece como entrada a otro nodo, pero también las instancias de computación virtual se comparten entre los nodos. El aumento de los nodos Fog en la colaboración P2P es bastante simple y los nodos se pueden hacer reutilizables. Sin embargo, los problemas relacionados con la confiabilidad y el control de acceso son predominantes en la colaboración nodal P2P [2].

### 2.5.3. MAESTRO ESCLAVO

En varios trabajos, la colaboración nodal basada maestro-esclavo ha sido mencionada de manera detallada. Por lo general, a través de la colaboración basada maestro-esclavo, un nodo maestro de niebla controla las funciones, la carga de

procesamiento, la administración de recursos, el flujo de datos, etc., de los nodos esclavos subyacentes. Además, el enfoque basado en maestro-esclavo junto con las interacciones nodales basadas en clúster y P2P pueden formar una red de colaboración híbrida dentro del entorno de computación de Fog. Sin embargo, en el procesamiento de datos en tiempo real debido a este tipo de descomposición funcional, los nodos de niebla maestros y esclavos requieren un gran ancho de banda para comunicarse entre sí [2].

## 2.6. MÉTRICAS PARA MEDIR LA CALIDAD EN EL SERVICIO

Para conocer la satisfacción del cliente y poder estandarizar se deben de seguir diferentes métricas para conocer el funcionamiento, éstas métricas serán abordadas a continuación:

### 2.6.1. TIEMPO

Este es un factor importante para medir la calidad en el servicio, debido a que las operaciones serán llevadas a cabo de manera local [2].

### 2.6.2. TIEMPO DE COMPUTACIÓN.

Se refiere al tiempo necesario para ejecutar una tarea, el tiempo de cálculo de una aplicación depende en gran medida de la configuración de recursos donde la aplicación se está ejecutando o la tarea se ha programado y se puede cambiar de acuerdo con la carga existente [24]. Para la comunicación en la niebla es importante conocer el tiempo en que ciertas aplicaciones están activas o inactivas ya que influyen significativamente en los recursos utilizados.

### 2.6.3. TIEMPO DE COMUNICACIÓN

Se define como el retardo en la red para intercambiar datos dentro de un entorno de niebla. En la literatura se ha discutido en 2 pliegues: dispositivo final / sensores para nodos de niebla [25], y nodos de niebla para nodos de niebla [24].

#### 2.6.4. LA FECHA LIMITE (DEADLINE)

Especifica el retardo máximo en la entrega del servicio que un sistema puede tolerar, la fecha límite para completar la tarea se ha considerado como un parámetro importante para medir la calidad de servicio (QoS) del sistema. Básicamente, el plazo de entrega de servicios desempeña un papel importante en la caracterización de aplicaciones sensibles a la latencia y tolerantes a la latencia. Además, se puede investigar el impacto de otras métricas basadas en el tiempo, como la frecuencia de detección de datos del dispositivo/sensores finales, la arquitectura de múltiples inquilinos del tiempo de acceso al servicio, el tiempo esperado de respuesta del servicio, etc., para el servicio eficiente y el aprovisionamiento de recursos en la computación de niebla [2].

### 2.7. DATOS.

A continuación, se describen las características de datos de entrada y flujo de datos para la computación en la niebla.

#### 2.7.1. TAMAÑO DE DATOS.

Se refiere a la cantidad de datos que deben ser procesados por la computación en la niebla, diferentes autores han relacionado el tamaño de los datos con respecto a los requisitos computacionales de las solicitudes [26]; de igual manera los datos recopilados por la niebla como dispositivos y sensores pueden contener características de Big data [17] en este sentido el tamaño de datos que controla la red juega un papel importante en la toma de decisiones.

#### 2.7.2. FLUJO DE DATOS

Define las características del flujo de datos a través del entorno fog, este entorno puede ser impulsado por eventos o en tiempo real, lo que influye en el servicio en gran medida [22], [27]. Además, el cambio repentino en el flujo de datos a veces promueve el equilibrio de carga dinámico entre los nodos [28].

## 2.8. COSTO

Como pasa en los diferentes productos y servicios, el costo depende principalmente del proveedor, así mismo pasa con el fog computing, el cual se divide en otros costos [2].

### 2.8.1. COSTO DE RED

La computación en la niebla se relaciona directamente con el ancho de banda y todo lo relacionado, en diversos trabajos los costos de carga de los dispositivos y sensores, el costo de intercambio de datos entre nodos se ha considerado como elemento de costo de red [19], mientras que en otros trabajos la latencia de red experimentada debido a problemas de ancho de banda se ha denominado costo de la red [29].

### 2.8.2. COSTO DE DESPLIEGUE

Este costo se relaciona directamente con el proveedor del servicio, requisitos del cliente, tamaño de niebla entre otros, ya que se define por la infraestructura usada para brindar el servicio como lo pueden ser algunos nodos, enrutadores, puertos de enlace entre otros, buscando la eficiencia en el servicio [2].

### 2.8.3. COSTO DE EJECUCIÓN

Este costo se mide después de que entra en operación los nodos de niebla mientras se ejecutan aplicaciones u operaciones de procesamiento. El costo total de ejecución se ha calculado en términos de tiempo de finalización de la tarea y costo de uso de recursos por unidad de tiempo [29].

También es importante tomar en cuenta que existen algunos gastos extras por cifrado, codificado y seguridad, al igual que el costo de algunas aplicaciones y servicios extras.

## 2.9. CONTEXTO

El contexto se refiere a la situación o condición de una determinada entidad en diferentes circunstancias.

### 2.9.1. USUARIO

El contexto del usuario, como las características, el historial de uso del servicio, la probabilidad de renuncia del servicio, etc., se pueden utilizar para asignar recursos para ese usuario en el futuro, por ejemplo, Net Promoter Score (NPS) y los requisitos del usuario también se pueden usar para fines de servicio y aprovisionamiento de recursos. En otros trabajos, la densidad de usuarios, la movilidad y el estado de la red también se han considerado para el aprovisionamiento de servicios.

### 2.9.2. APLICACIÓN

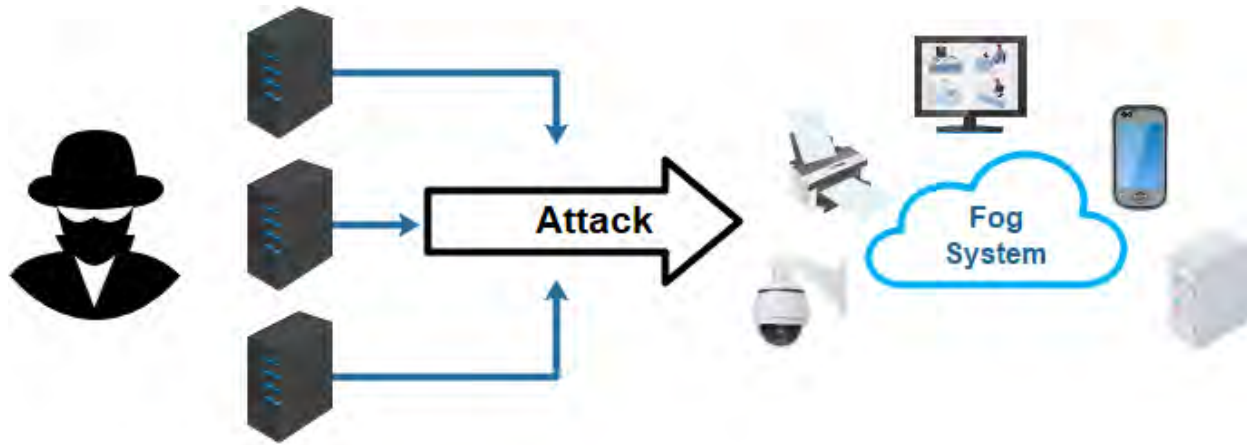
El contexto de la aplicación puede considerarse como requisitos operativos de diferentes aplicaciones. Los requisitos operativos incluyen requisitos de procesamiento de tareas (velocidad de CPU, almacenamiento, memoria), requisitos de red, etc., y pueden afectar el aprovisionamiento de recursos y servicios. En otros trabajos, la carga de tareas actual de diferentes aplicaciones también se ha considerado como contexto de aplicación, Además, la información contextual en la computación de niebla puede discutirse en términos de entorno de ejecución, características nodales, arquitectura de aplicaciones, etc. y junto con los otros contextos pueden desempeñar papeles vitales en el aprovisionamiento de recursos y servicios. Por lo tanto, es esencial investigar el impacto de cada información contextual en detalle [2].

## 2.10. CONSUMO ENERGÉTICO Y HUELLA DE CARBONO

En la actualidad, el cuidado del medio ambiente y el uso eficiente de los recursos ha tomado esencial relevancia, y para la computación en la niebla no es una excepción, al comparar el consumo de energía de la niebla con la nube, este viene siendo en menor escala, por lo que se puede considerar de bajo consumo energético, de igual manera su consumo energético puede ser optimizado por la misma red. Seguridad en la niebla hoy en día dentro de la nube e internet se desarrolla cada día más con el propósito de brindar un servicio seguro y de calidad, pero de igual manera los sistemas de hackeo



evolucionan y pueden ser una potencial amenaza para la computación en la nube, la vulnerabilidad de seguridad de la computación en niebla es muy alta, ya que reside en la red subyacente entre los dispositivos / sensores finales y los centros de datos de la nube. Sin embargo, las preocupaciones de seguridad en la computación de niebla se han discutido en términos de autenticación de usuarios, privacidad, intercambio de datos seguro, ataque DoS [2].



*Ilustración 6 Seguridad en la niebla*

### 2.11. OBJETIVOS DE LA COMPUTACIÓN EN LA NIEBLA

Los objetivos de servicio para la computación en la niebla vienen dados por las necesidades del cliente, por lo que se busca tener un buen control de los sistemas de niebla, por esta razón se desarrollaron los siguientes términos para medir la calidad en el servicio, se han propuesto varias arquitecturas únicas de nodo de niebla, plataforma de programación de aplicaciones, modelo matemático y técnica de optimización para lograr ciertos SLO [2].



Ilustración 7 Gestión de recursos

## 2.12. GESTIÓN DE LA LATENCIA

Como principal objetivo de esta gestión es reducir el tiempo de respuesta, el cual debe ser definido por el prestador del servicio, la administración de latencia en la computación de niebla básicamente resiste el tiempo de entrega de servicio máximo de superar un umbral aceptado. Este umbral puede ser la latencia máxima tolerable de una solicitud de servicio o el requisito de QoS de las aplicaciones, para esto se debe de llevar a cabo el control de los nodos de niebla de manera eficiente para usar el más conveniente dependiendo la ubicación del usuario [2].

### 2.13. GESTIÓN DEL COSTO

Para definir el costo de ese servicio hay que entender que depende directamente del proveedor y del área en la cual se va a instalar, el proveedor define el costo de los nodos, la instalación y el precio de mantenimiento. Mientras que el lugar mediante el tamaño define el número de nodos a utilizar y su ubicación puede necesitar protección. La administración de costos en la computación en niebla se puede discutir en términos de gastos de capital (Capital Expenses CAPEX) y gastos de operación (Operating Expenses OPEX). El principal contribuyente de CAPEX en la computación de niebla es el despliegue del costo de los nodos de niebla distribuidos y sus redes asociadas. En este caso, la ubicación adecuada y el número optimizado de nodos fog desempeñan un papel importante en la minimización del CAPEX en la computación de la niebla [2].

### 2.14. GESTIÓN DE RED

Esta gestión sirve principalmente para el control de la gestión de la red principal, esto a través de diversos soportes que se explicarán a continuación:

#### 2.14.1. CONGESTIÓN DE RED

Este problema se genera principalmente debido al aumento de la sobrecarga en la red. Al igual que en IoT, los dispositivos / sensores finales están altamente distribuidos a lo largo del borde, las interacciones simultáneas de los componentes finales con los centros de datos de la nube pueden aumentar la sobrecarga en la red central en gran medida. En tal caso, se producirá una congestión de la red y se degradará el rendimiento del sistema. Teniendo en cuenta este hecho, en una arquitectura en capas del nodo de niebla se ha propuesto implementar un procesamiento local de las solicitudes de servicio. Como consecuencia, a pesar de recibir solicitudes de servicio masivas, las clouds obtienen una versión consensuada de las solicitudes que contribuyen menos a la congestión de la red.

Este problema se genera principalmente por el alto número de dispositivos que están conectados a la red, los cuales están distribuidos alrededor del borde lo que puede

afectar el rendimiento del sistema. Por este se hecho se ha propuesto una arquitectura por capas, proporcionando procesamiento local de las solicitudes de servicio [21].

#### 2.14.2. VIRTUALIZACIÓN

Para la virtualización, las redes definidas por software son de gran utilidad, ya que desacoplan el plano de control implementando el uso de servidores separados.

La virtualización del sistema de red convencional ya ha atraído una significativa atención de la investigación. SDN se considera uno de los habilitadores claves de la red virtualizada. SDN es una técnica de red que desacopla el plano de control de los equipos de red e implementa el software en servidores separados. Uno de los aspectos importantes de SDN es proporcionar soporte para NFV. Básicamente, NFV es un concepto arquitectónico que virtualiza las funciones de red tradicionales (traducción de direcciones de red (NAT), firewalls, detección de intrusos, servicio de nombres de dominio (DNS), almacenamiento en caché, etc.) para que puedan ejecutarse a través del software [22].

#### 2.14.3. CONECTIVIDAD

Este apartado es de suma importancia, ya que en este tipo de redes más cercanas a los usuarios es necesario que los dispositivos tengan una mejor conexión entre ellos sin importar su tipo, por eso es necesario desarrollar una arquitectura segura que mejore la comunicación de los dispositivos máquina a máquina. Garantiza una comunicación perfecta de los dispositivos finales con otras entidades como Cloud, Fog, computadoras de escritorio, dispositivos móviles, dispositivos finales, etc., a pesar de su diversidad física. Como consecuencia, el descubrimiento de recursos, el mantenimiento de la comunicación y la capacidad de cómputo se hacen más fáciles dentro de la red [2].



Ilustración 8 conectividad

## 2.15. GESTIÓN DE LA COMPUTACIÓN

Para la gestión de los recursos en la computación en la niebla, incluyendo la distribución de recursos, asignación de trabajo y coordinación.

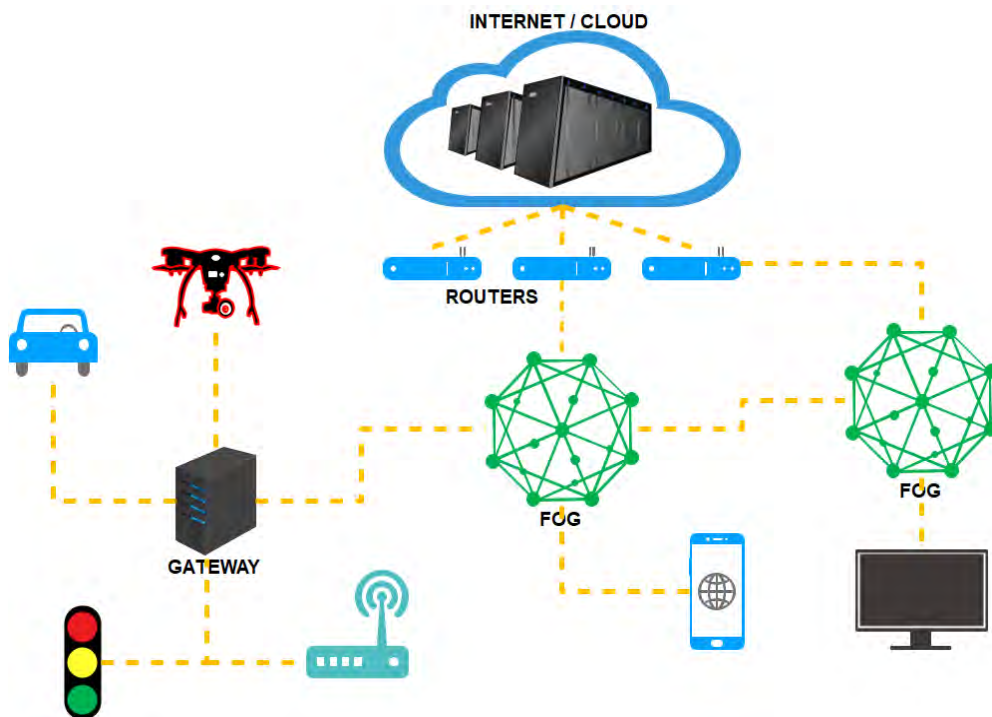


Ilustración 9.- Fog managment

### 2.15.1. DISTRIBUCIÓN DE RECURSOS

Fog computing ayuda a asignar recursos computacionales de acuerdo con algunas políticas para que se puedan asignar los recursos apropiados para cálculos adicionales, se puede lograr la QoS deseada y un precio de servicio preciso se puede imponer. Esta gestión consiste en la asignación de recursos de acuerdo a políticas de las empresas para asignar un servicio de calidad a los usuarios de la computación en la niebla [22], [23].

### 2.15.2. ASIGNACIÓN DE CARGA DE TRABAJO

Este es un método de optimización de la niebla, en el cual se busca maximizar la utilización del servicio y minimizar los tiempos donde no se ocupa, para de esta manera ofrecer en los dispositivos del cliente un servicio de calidad. En fog computing debe realizarse de tal manera que la tasa de utilización de los recursos se maximice y el período de inactividad computacional más largo se minimice, para ser más precisos, se asegura una carga equilibrada en diferentes componentes.

### 2.15.3. COORDINACIÓN

Para un sistema heterogéneo, descentralizado y de recursos limitados la coordinación juega con un papel importante, que las aplicaciones ejecutadas se distribuyen en los diferentes nodos de niebla, por lo que la falta de coordinación puede afectar en el rendimiento del sistema.

## 2.16. ADMINISTRACIÓN DE APLICACIONES

Para garantizar una gestión adecuada de las aplicaciones en la computación de niebla, las plataformas de programación eficiente son muy esenciales. Además de la escalabilidad y la facilidad de descarga de computación, también contribuyen significativamente en la administración de aplicaciones [2]. Para el uso de aplicaciones en la computación en la niebla, es necesario el desarrollo de plataformas, estaciones de descarga para poder para desarrollar, compilar y ejecutar aplicaciones. Esto se ha convertido en un desafío para la computación en la nube, por lo que se diseñó una plataforma para su naturaleza dinámica, llamada "mobile fog" la cual ofrece una

abstracción simplificada de los modelos de programación para el desarrollo a gran escala [16].

#### 2.16.1 PLATAFORMA DE PROGRAMACIÓN (PROGRAMMING PLATFORM)

Proporciona los componentes necesarios, como interfaces, bibliotecas, entorno de tiempo de ejecución, etc., para desarrollar, compilar y ejecutar aplicaciones. Debido a la naturaleza dinámica de la computación en niebla, la garantía de un soporte de programación adecuado para aplicaciones a gran escala es muy desafiante. Para superar este problema, se ha introducido una nueva plataforma de programación llamada Mobile Fog. Mobile Fog ofrece una abstracción simplificada de los modelos de programación para desarrollar aplicaciones a gran escala sobre dispositivos distribuidos de forma heterogénea. En otro papel, además de coordinar los recursos durante la ejecución de las aplicaciones, también se diseñó una plataforma de programación basada en el enfoque de flujo de datos distribuidos para el desarrollo de aplicaciones en la computación en niebla [2].

#### 2.16.2. ESCALAMIENTO “AJUSTE” (SCALING).

Apunta a la capacidad de adaptación de las aplicaciones en la retención de su calidad de servicio, incluso después de la proliferación de los usuarios de aplicaciones y eventos impredecibles. Las técnicas de escalado también se pueden aplicar en la programación de aplicaciones y el acceso al servicio de los usuarios. Para admitir la programación escalable de las aplicaciones de flujo de datos, la arquitectura de un planificador autoadaptativo con reconocimiento de QoS se ha propuesto recientemente en la computación de niebla. Este programador puede escalar aplicaciones con el aumento de usuarios y recursos, y no solicita información global sobre el entorno. Además, debido a la capacidad auto adaptativa del programador, la reconfiguración automática de los recursos y la colocación de las aplicaciones de forma distribuida se vuelven más fáciles. Además, en función de la distancia, la ubicación y los requisitos de QoS de las entidades de acceso al servicio, también se ha propuesto una técnica adaptativa para la selección del modo de acceso de servicio de los usuarios en el cómputo de niebla [2].

### 2.16.3. TÉCNICAS DE DESCARGA (OFFLOADING)

Facilita que los dispositivos finales con recursos limitados envíen sus tareas informáticas a algunos dispositivos enriquecidos con recursos para su ejecución. La descarga computacional es un entorno de nube inmóvil muy común. Sin embargo, recientemente, como parte de la mejora de la compatibilidad de la computación en niebla para otros sistemas de redes, el soporte de descarga de computación para aplicaciones móviles en la computación en niebla se ha enfatizado en varios artículos [2].

### 2.17. GESTIÓN DE DATOS

La gestión de los datos es de vital importancia para un servicio de calidad, ya que no todos los datos son enviados a la nube y se tienen que procesar localmente, se debe de hacer una buena distribución de los nodos de niebla para un eficaz almacenamiento.

### 2.18. GESTIÓN DE ENERGÍA

Es importante resaltar que, desde el punto de vista ecológico, la computación en la niebla se puede considerar una red verde, ya que puede ser utilizada para el control de la energía derivado de los objetos conectados, aunque el beneficio no es exclusivamente de las pequeñas redes de niebla, sino también la nube se ve beneficiada al no ejecutar aplicaciones que generan mayor consumo energético, las cuales son ejecutadas en la niebla [2].

### 2.19. SISTEMA DE RED APLICABLE

La computación en niebla juega un papel importante en IoT. Sin embargo, en trabajos de investigación recientes, también se ha destacado la aplicabilidad de la informática de niebla en otros sistemas de red (red móvil, red de distribución de contenido, red de acceso de radio, red de vehículos, etc.) [2].

### 2.20. IOT

En IoT, todos los dispositivos están interconectados y pueden intercambiar datos entre ellos. El entorno de IoT se puede describir desde diferentes perspectivas. Además



de especificar IoT como una red para la interacción de dispositivo a dispositivo, en varias investigaciones basadas en fog, esta interacción se ha clasificado en la industria y el entorno de ejecución basado en el hogar. Además, la red de sensores y actuadores inalámbricos, los sistemas ciber físicos, la red de sistemas integrados, etc. también se han considerado como diferentes formas de IoT al diseñar modelos de sistemas y servicios para la computación de niebla [2].

## 2.21. MOBILE NETWORK / RAN

La red móvil es otro sistema de red donde se ha explorado la aplicabilidad de la computación de niebla a través de varios trabajos de investigación. Básicamente, se ha puesto mucho énfasis en investigar la compatibilidad de la computación de niebla en las redes móviles 5G; 5G permite una comunicación de mayor velocidad, capacidad de señal y una latencia mucho menor en la prestación de servicios en comparación con los sistemas celulares existentes. Además de 5G, la computación de niebla también se puede aplicar en otras redes móviles como 3G, 4G, etc. Además, se investigó en detalle la asignación de carga de trabajo impulsada por un intercambio de energía en Fog-Cloud para la comunicación basada en dispositivos móviles. Radio Access Network (RAN) facilita la comunicación de dispositivos individuales con otras entidades de una red a través de conexiones de radio. La RAN asistida en la nube llamada CRAN ya ha atraído mucha atención de investigación. Para complementar CRAN, también se ha explorado la potencialidad de la red de acceso de radio basada en la computación de niebla [2].

## 2.22. RED ÓPTICA PASIVA DE LARGO ALCANCE / COMUNICACIÓN DE LÍNEA DE ALIMENTACIÓN (LRPON / PLC)

### 2.22.1 LA RED ÓPTICA PASIVA DE LARGO ALCANCE (LRPON)

Se ha introducido para admitir servicios de retroceso orientados al hogar, a la industria e inalámbricos, sensibles a la latencia e intensivos en ancho de banda. Además, cubriendo un área grande, los LRPON simplifican el proceso de consolidación de la red. En fog computing se ha integrado con LRPON para un diseño de red optimizado [2].

### 2.22.2 LA COMUNICACIÓN POR LÍNEA ELÉCTRICA (PLC)

La comunicación por línea eléctrica (PLC) es un método de comunicación ampliamente utilizado en Smart Grid. En el PLC, utilizando el cableado eléctrico, tanto los datos como la corriente alterna (CA) se transmiten simultáneamente [2].

### 2.23. RED VEHICULAR

La red vehicular permite la creación autónoma de una comunicación inalámbrica entre vehículos para el intercambio de datos y el aumento de recursos. En este sistema de red, los vehículos cuentan con instalaciones informáticas y de red. En varias investigaciones del tema, los vehículos que residen en la red de borde se consideran nodos de niebla para promover la red vehicular basada en la computación de niebla [2].

### 2.24. RED DE DISTRIBUCIÓN DE CONTENIDO (CDN)

Se compone de servidores proxy distribuidos que proporcionan contenido a los usuarios finales asegurando un alto rendimiento y disponibilidad. En varias investigaciones basados en fog, los nodos de fog se consideran servidores de contenido para admitir la distribución de contenido a través de la informática de fog. Dado que los nodos se colocan de manera distribuida en el borde de la red, los usuarios finales pueden acceder a los servicios de contenido basados en la tecnología con un retraso muy mínimo. Como consecuencia, será más fácil garantizar un alto rendimiento en la distribución de contenido [2].

### 2.25. SEGURIDAD EN LA NIEBLA.

#### 2.25.1. AUTENTIFICACIÓN

La autenticación de los usuarios en servicios basados en fog juega un papel importante en la resistencia a la intrusión. Dado que los servicios de fog se utilizan en forma de "pago por uso", el acceso no deseado a los servicios no es tolerable en ningún sentido. Además de la autenticación de usuarios, la autenticación de dispositivos, la autenticación de migración de datos y la autenticación de instancias también se han observado en el entorno de computación la protección de fog. Los dispositivos

conectados a la niebla pueden enfrentar problemas de autenticación, lo cual no pasa en la nube, pero no se puede usar este servicio de la nube debido a que la autenticación debe seguir trabajando para acceder a los dispositivos del personal localmente cuando la autenticación es remota [31].

### 2.25.2. CIFRADO

Básicamente, la computación en niebla complementa la computación en nube. Los datos que se han procesado en la computación de niebla, en algunos casos se tienen que reenviar a la nube. Como estos datos a menudo contienen información confidencial, es muy necesario cifrarlos en los nodos de fog. Teniendo en cuenta este hecho, se ha incluido una capa de cifrado de datos en la arquitectura del nodo fog propuesta [2].

### 2.25.3. PRIVACIDAD

La computación de niebla procesa los datos procedentes de dispositivos / sensores finales. En algunos casos, estos datos se encuentran muy relacionados con la situación y el interés de los usuarios. Por lo tanto, una garantía de privacidad adecuada es considerada como una de las preocupaciones de seguridad importantes en la computación de la niebla. En los desafíos relacionados con la privacidad en la niebla, la computación vehicular basada ha sido señalada para una mayor investigación [2].

### 2.25.4. ATAQUE DOS

Dado que, los nodos de niebla son una restricción de recursos, es muy difícil para ellos manejar un gran número de solicitudes simultáneas. En este caso, el rendimiento de la computación en niebla se puede degradar en gran medida. Para crear interrupciones de servicio tan severas en la computación en niebla, los ataques de denegación de servicio (DoS) pueden desempeñar funciones vitales. Al hacer muchas solicitudes de servicio irrelevantes simultáneamente, los nodos de niebla pueden estar ocupados por un período de tiempo más largo. Como resultado, los recursos para hospedar servicios útiles dejan de estar disponibles [2].

## CAPITULO 3. APLICACIONES

La tecnología avanza día a día y cada vez la necesidad de sistemas más rápidos y potentes se vuelve latente, mediante el constante avance del internet y la cuarta revolución industrial cada días más personas se conectas a internet mediante diferentes aparatos de uso diario como celulares, tabletas o laptops, esto desde su casa u oficina, pero al igual de esta manera los datos se conectan a internet sin tener que ser operados como son los sensores, electrodomésticos o maquinas, los cuales trabajan mediante la nube, pero este recurso suele no satisfacer las necesidades actuales del internet de las cosas por la saturación en el manejo de datos, a esta solución se propone la computación en la niebla y se describen algunos ejemplos de funcionamiento.

### 3.1. COMPUTACIÓN DE NIEBLA VEHICULAR

Los sistemas vehiculares inteligentes se basan en muchos programas sofisticados y uno de los principales entre ellos es el Vehicular Ad-hoc Networks (VANET). VANET garantiza la eficiencia del tráfico, la seguridad y la comodidad de conducción mediante el intercambio de información. Básicamente, VANET se destaca en el intercambio de información y trae consigo varios beneficios, como la seguridad, la conveniencia, la eficiencia de conducción. VANET facilita varios servicios móviles que, entre otros, incluyen el servicio de difusión de datos que resulta útil. durante situaciones críticas como emergencias, aplicaciones de distribución de contenido que son útiles para medios, entretenimientos, anuncios, etc. En los últimos años, VANET ha sido testigo de un crecimiento fenomenal, sin duda ayudado por la llegada de nuevos avances y el desarrollo de equipos y tecnologías. Al mismo tiempo, este avance de las tecnologías suscitó una nueva preocupación: una creciente demanda de comunicación de información y una mayor capacidad de cómputo. Las aplicaciones más nuevas han fomentado expectativas y demandas. Por ejemplo, las aplicaciones como la conducción autónoma, la realidad aumentada (AR) que se basan en el procesamiento de datos y el trabajo de almacenamiento, complicando ahora necesitan grados más avanzados de comunicación, procesos computacionales y capacidades de almacenamiento [3].

### 3.2. CIUDADES INTELIGENTES

Para entender cómo funciona la computación en la niebla en una ciudad inteligente primero debemos de definir este término: Chourani las define así *“Combinación cada vez más eficaz de las redes digitales de telecomunicaciones, la inteligencia integrada de forma ubicua, sensores, etiquetas y software”* [8]. En este sentido el recurso tecnológico a usar, es la creación de la computación en la niebla que abarque toda la ciudad, teniendo como nodos cualquier dispositivo electrónico dentro de la ciudad, o hasta un vehículo inteligente.

Para esto debemos buscar una posible aplicación en una ciudad conectada al internet, por ejemplo: al crear una smart city todos los vehículos que circulan por las calles, así como todos los semáforos y sensores de tráfico estarían conectados simultáneamente a una red local (ver *ILustración 10*), en la cual la información se procesaría de manera local y rápida para detectar accidentes, embotellamientos o problemas en las calles. De esta manera se podría agilizar las vialidades y servir de gran ayuda para prevenir accidentes y ayudar a los servicios de seguridad a llegar más rápido a cualquier lugar dentro de la ciudad [4].



*Ilustración 10 Smart city*

Otra aplicación en las ciudades inteligente es el uso de los recursos disponibles, un ejemplo sería el uso eficiente de los recursos naturales, como la iluminación de las calles de la ciudad, esto implicaría que toda la luminaria esté conectada a una red de niebla, la cual controle la intensidad de las lámparas por medio de sensores, o desconectarla si a ninguna persona le es de ayuda, todo esto de una más rápida y eficiente [4].

### 3.3. AUTOPISTAS INTELIGENTES.

Otra futura aplicación de la computación en la niebla son las autopistas inteligentes, en las cuales, sus principales nodos de transmisión serían los vehículos conectados a internet, y algunas cámaras y sensores instalados a lo largo de la carretera, de esta manera se podrá conocer el status constante de la vía y poder ejecutar un plan de reacción en caso de que se presente algún tipo de accidente, deslave o conocer el desgaste.

También existen otro tipo de aplicaciones en las carreteras inteligentes, esto debido al uso de autos autónomos, los cuales son capaces de prevenir y detectar posibles accidentes desde una comunicación máquina- máquina esto por medio de todos los autos autónomos que circulen en una misma red [4].

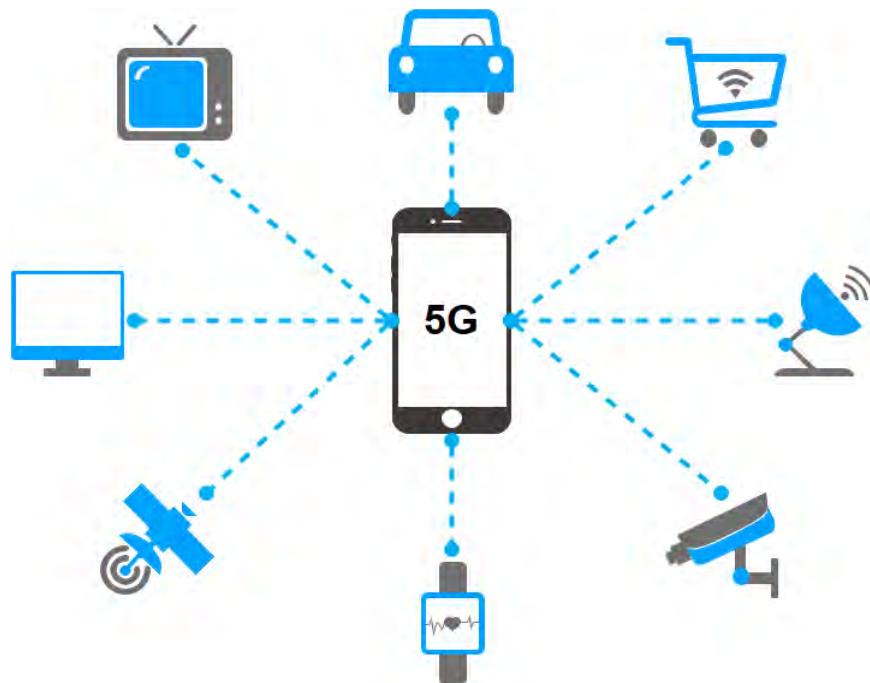
### 3.4. TELEFONÍA 5G

Al igual que en las diferentes áreas, en las telecomunicaciones es posible hacer uso de la computación en la niebla, esto puede ser llevado a cabo para las compañías y usuarios, permitiendo que los dispositivos conectados puedan fungir como nodos de niebla, esto traería beneficios respecto a la baja latencia y la escalabilidad, por medio de tres principales componentes, nodos escalables, controladores y el servicio brindado por las compañías de telecomunicaciones [9].

Como se ha mencionado anteriormente en los tipos de nodos, la mayoría de estos permanecen estáticos, aunque como los vehículos pueden existir algunos nodos que estén en movimiento, por lo que se creó la computación en la niebla portátil, aunque los nodos de niebla portátiles presentan un mayor desafío pueden presentar un mayor

beneficio para el entorno fog, mejorando la calidad del servicio, costo y consumo energético.

Existen nuevos métodos de aprovisionamiento para servicios de niebla móviles, de modo que los servicios de niebla están disponibles para los nodos y usuarios de IoT.



*ilustración 11 fog mobile nodes*

Para continuar garantizando la sostenibilidad de los servicios de comunicaciones móviles durante la próxima década y para satisfacer las demandas de los negocios y los consumidores, se espera que los servicios de comunicaciones móviles de quinta generación (5G) se implementen para 2020. Uno de los principales requisitos para las redes 5G es la mejora significativa de la eficiencia espectral (SE) en comparación con la cuarta generación (4G), ya que el aumento exponencial anticipado en el volumen de tráfico de datos móviles es enorme, por ejemplo, al menos 1,000 veces en la década de 2020 en comparación con 2010. En particular, la velocidad máxima de datos en 5G debe ser 10-20 Gbps que es 10-20 veces la velocidad máxima de datos en 4G, y la velocidad de datos experimentada por el usuario debe ser de 1 Gbps (100 veces la velocidad de

datos experimentada por el usuario en 4G). Además, el rápido desarrollo de Internet móvil e Internet de las cosas (IoT) exponencialmente acelera las demandas de aplicaciones de alta velocidad de datos, que incluyen transmisión de video de alta calidad, redes sociales y comunicaciones de máquina a máquina [5].

#### 3.4.1. FOG COMPUTING UN REQUERIMIENTO PARA LAS REDES 5G

Se espera que las redes móviles 5G, aunque no sean una realidad en la actualidad, lleguen al mercado para 2020. La comunicación en las redes 5G se basará en señales de alta frecuencia, en la banda de frecuencia de onda milimétrica, que puede asignar más ancho de banda para entregar contenido de video y multimedia más rápido y de mayor calidad. Las redes 5G prometen proporcionar una latencia de milisegundos y submilisegundos al tiempo que ofrecen una velocidad de datos de más de 1 Gbit/s. Esta latencia es tan pequeña que elimina la posibilidad de que la interfaz de radio sea el cuello de botella. Las redes móviles de próxima generación están diseñadas de una manera que puede manejar las comunicaciones no restringidas a los humanos (donde uno puede enmascarar la latencia), están construidas para soportar también una comunicación confiable y rápida de máquina a máquina, un caso de uso que necesita baja latencia para ser efectivo [5].

#### 3.4.2. ARQUITECTURA DE RED FÍSICA

La arquitectura de red física de una red de niebla sobre 5G extenderá la arquitectura de las redes de acceso de radio en la nube heterogénea (HCRAN) de última generación. En la arquitectura tradicional de HCRAN, todas las tareas de procesamiento de aplicaciones se realizan en la nube dentro de la red central, lo que requiere miles de millones de dispositivos finales para comunicar sus datos a la red central. Tal cantidad masiva de comunicación puede sobrecargar la capacidad de fronthaul y puede sobrecargar la red central, lo que tendrá un impacto perjudicial en la QoS experimentada por los usuarios finales [5].



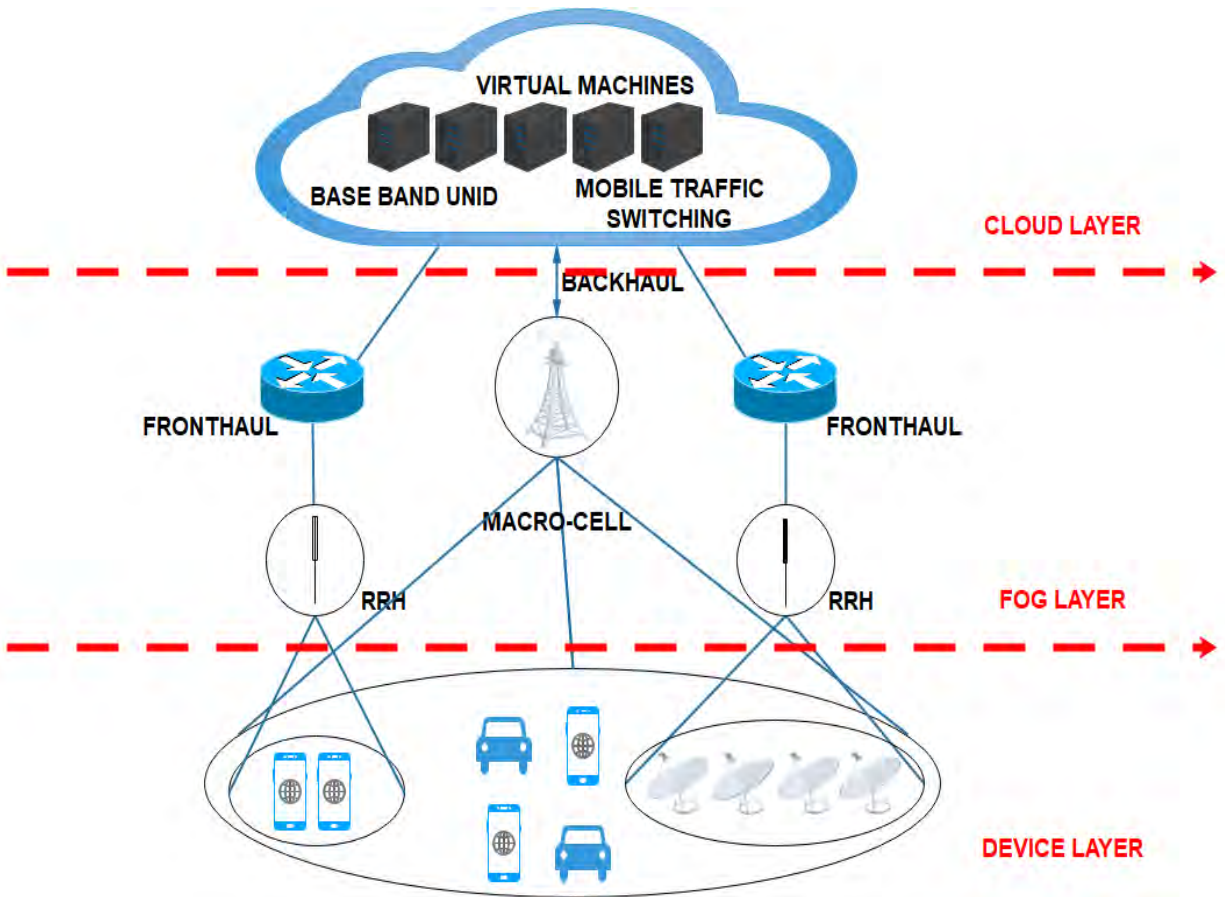


Ilustración 12.- Arquitectura de red 5G

Una solución intuitiva a este problema es reducir las capacidades de cómputo y almacenamiento desde la nube cerca del borde, de modo que la necesidad de enviar todos los datos generados por los dispositivos finales a la nube se solucione, por lo tanto, aliviando el fronthaul y el núcleo red de la inmensa oleada de tráfico. La Ilustración 12. muestra las diversas ubicaciones donde se puede realizar esta descarga de cómputo y almacenamiento. La arquitectura de la red de niebla consta de tres capas lógicas que se muestran en la Ilustración 12. Los dispositivos en cada capa son capaces de alojar computación y proporcionar almacenamiento, lo que permite crear políticas complejas de descarga de procesamiento [5].

### 3.4.3. CAPA DEL DISPOSITIVO

La capa del dispositivo subsume todos los dispositivos finales conectados a la red de niebla. Los dispositivos incluyen dispositivos IoT como sensores, puertas de enlace y otros, y también dispositivos móviles como teléfonos inteligentes, tabletas y otros. Estos dispositivos pueden estar intercambiando datos directamente con la red, o pueden estar realizando comunicación entre pares. Siendo la fuente de todos los datos que ingresan a la red y los actuadores principales que realizan tareas, estos dispositivos son el nivel más bajo de dispositivos de niebla. La capa del dispositivo aloja el cómputo ya sea mediante codificación integrada (para dispositivos de gama baja como sensores) o como un software que se ejecuta en el sistema operativo del dispositivo [5].

### 3.4.4. CAPA DE NIEBLA

La capa de niebla consta de dispositivos de red intermedios ubicados entre los dispositivos finales en la capa de dispositivos y la capa de nubes. El primer punto de descarga en esta capa son los cabezales de radio remotos (RRH) y las celdas pequeñas que están conectadas por fibra de fronthaul a la red central. El procesamiento de datos entrantes aquí reducirá considerablemente la carga en el fronthaul. Las macro celdas también forman un punto de procesamiento de descarga que envía los datos procesados a la red central a través de enlaces de retorno. Tanto el fronthaul como el backhaul se realizan mediante enlaces Ethernet y los dispositivos intermedios como el enrutador y los conmutadores en el camino desde los cabezales de radio hasta el núcleo también forman lugares potenciales donde se pueden descargar las tareas de computación y almacenamiento [5].

La implementación de aplicaciones en estos dispositivos es posible gracias a los avances en la tecnología de virtualización. Cada aplicación se empaqueta en forma de máquina virtual y se inicia en el dispositivo apropiado. Las máquinas virtuales de la aplicación se ejecutan junto con la máquina virtual del sistema operativo host (que realiza las operaciones de red originales) a través de un hipervisor en el dispositivo de niebla [5].

#### 3.4.5. CAPA DE NUBE

Esta capa forma el vértice de la arquitectura jerárquica, siendo las máquinas virtuales de nube los puntos de descarga de cómputo. La escalabilidad teóricamente infinita y la infraestructura de gama alta de la nube hacen posible manejar el procesamiento que requiere una computación intensiva y un gran almacenamiento, que no se puede hacer en los dispositivos de borde. Además del procesamiento de la capa de aplicación, la capa de la nube contiene unidades de banda base que procesan datos provenientes de RRH y celdas pequeñas a través de fronthauls y enrutan los datos procesados a los servidores de aplicaciones [5].

#### 3.4.6. ARQUITECTURA DE LA APLICACIÓN

Para que una aplicación se llame preparada para niebla, debe estar diseñada para aprovechar todo el potencial de la niebla. Por lo general, una aplicación creada para su ejecución en infraestructura de niebla tendría tres componentes: dispositivos, componentes de niebla y nube [5].

#### 3.4.7. COMPONENTE DEL DISPOSITIVO

El componente del dispositivo está vinculado a los dispositivos finales. Realiza operaciones a nivel de dispositivo, principalmente, administración de energía, eliminación de redundancia y otros. A veces, cuando el dispositivo final no es solo un cliente ligero, también aloja la lógica de la aplicación que exige respuestas de muy baja latencia, ya que este componente se ejecuta en el dispositivo mismo. Sin embargo, debido a las limitaciones de recursos del dispositivo subyacente, este componente no debe contener tareas de procesamiento pesadas [5].

#### 3.4.8. COMPONENTE DE NIEBLA

El componente de niebla de una aplicación realiza tareas que son críticas en términos de latencia y requieren una potencia de procesamiento que los dispositivos finales no pueden proporcionar. Además, dado que el componente de niebla se debe ejecutar en dispositivos de niebla cerca del borde, la cobertura de este componente no

es global. Por lo tanto, este componente debe alojar una lógica que requiera solo información de estado local para ejecutarse.

El componente de niebla no está vinculado a un tipo particular de dispositivo. Es libre de residir en cualquier tipo de dispositivo entre el borde (que consiste en dispositivos finales) y la nube. La asignación de los componentes de niebla a los dispositivos depende de los puntos de descarga en el camino desde el borde hasta la nube. Dependiendo de la cobertura geográfica y los requisitos de latencia de la aplicación, el componente de niebla se puede alojar en cualquiera de estos puntos de descarga. De hecho, la colocación del componente de niebla en los nodos apropiados forma un área interesante e importante para la investigación [5].

#### 3.4.9. COMPONENTE DE LA NUBE

El componente de la nube está limitado a los servidores de la nube en la red central. Contiene lógica para el análisis a largo plazo de los datos recopilados de las capas inferiores y para operaciones que no tienen ningún tipo de restricciones de latencia. Las tareas de aplicación que requieren gran capacidad de procesamiento y almacenamiento son adecuadas para colocarse en el componente de la nube, de modo que puedan aprovechar los recursos infinitos de la nube. Además, como la capa de nube se encuentra en el vértice de la red, recibe información de todos los dispositivos y por lo tanto tiene un conocimiento global de todo el sistema. Por lo tanto, la lógica de la aplicación que requiere el conocimiento del estado global del sistema debe colocarse en el componente de la nube de la aplicación [5].

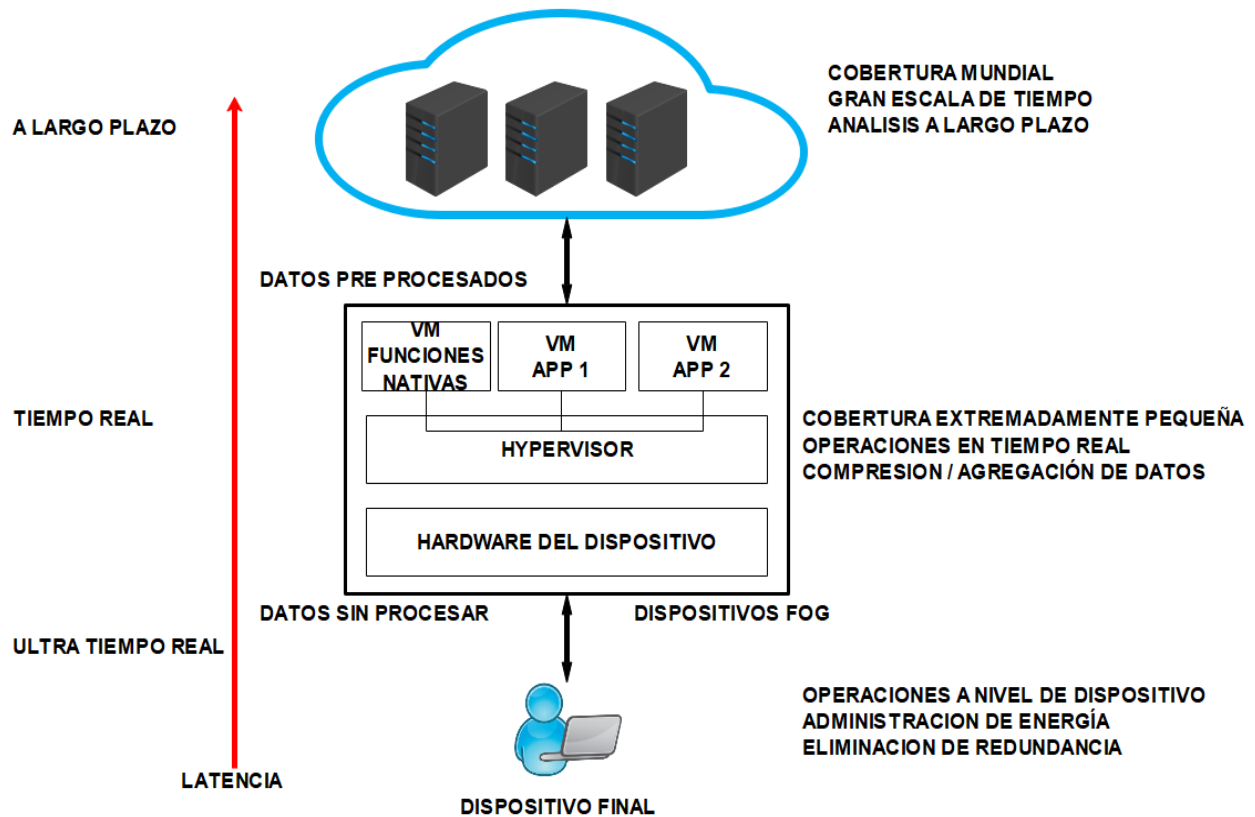


Ilustración 13.- Arquitectura de aplicación

### 3.5. CUIDADO DE LA SALUD

La atención médica es el área en la que se han citado con más frecuencia las aplicaciones basadas en la informática de niebla. En los últimos años, una amplia gama de servicios de salud y trabajos relacionados con el diagnóstico, detección de enfermedades de la salud etc. han sido propuestas [6].

Tabla 1.- Comparación entre diferentes sistemas de salud basados en fog

Nombre del marco.	Enfermedad monitorizada.	Técnica utilizada.	Software de dispositivos.	Fuente abierta.
AST.	Accidente cerebrovascular (ataque cerebral)	Detección de caídas.	Teléfonos inteligentes, Servidores en la nube.	No.

eWALL.	EPOC, demencia leve, enfermedades relacionadas con el envejecimiento.	Monitoreo de actividad diaria, monitoreo de funcionamiento diario.	Sensores, actuadores, nube eWALL, middleware en la nube.	No.
Health Fog.	Propósitos múltiples.	Reconocimiento de actividad, agente de seguridad de acceso a la nube.	Teléfonos inteligentes, dispositivos domésticos inteligentes, sensores portátiles.	No.
fHealth.	Fitness.	Seguimiento de actividad.	Teléfonos inteligentes, Servidores en la nube.	Si.

### 3.6. REALIDAD AUMENTADA, INTERFAZ DE MAQUINA DE CEREBRO Y JUEGOS

La realidad aumentada es una tecnología que combina la realidad virtual con el mundo real en forma de imágenes de video en vivo que se mejora digitalmente con gráficos generados por computadora. AR puede experimentarse a través de auriculares que usan las personas y mediante pantallas en dispositivos móviles. Hoy en día, decenas de empresas están adoptando la tecnología de Realidad Aumentada (AR) para vender sus productos y también producir estrategias de marketing y publicidad llamativas. Aplicaciones que confían en la tecnología AR, invariablemente se requiere un gran ancho de banda para transferir datos y computación de alta potencia para transmitir video en vivo. Esto se debe principalmente a que incluso un retraso de corta duración o un almacenamiento intermedio como la interrupción puede estropear la presentación para

los usuarios e invitar a la censura. Por lo tanto, para AR que usan aplicaciones, como algunas relacionadas con el cerebro en la atención de la salud, la baja latencia es una necesidad, y la computación de niebla resulta ser la mejor plataforma que podría cumplir con esta condición [1], [6].

### 3.7. RED DE ENERGÍA INTELIGENTE

La red de energía es una red de difusión energética; utiliza medidores inteligentes en diferentes áreas para cuantificar los datos de estado en curso, en lo que se refiere a la producción de energía, transporte, utilización y carga. La energía inteligente alude a la utilización de los avances de la administración de sistemas y la IoT para diseminar progresivamente la energía con un objetivo final específico para limitar su costo y también expandir energía, que incluye el liderazgo básico en términos de toma de decisiones y un subsistema de actuación de acción. Un servidor principal consolidado denominado marco de control de supervisión y adquisición de datos (SCADA) acumula y disecciona los datos de estado. Luego, para equilibrar la red eléctrica, transmite órdenes para reaccionar ante cualquier solicitud de cambio o crisis [6].

Por ejemplo, la mayor utilidad abierta en los EE. UU., Los Angeles Smart Grid atenderá a más de 4 millones de clientes [44]. Los medidores inteligentes conectados a la red vigilan el consumo de energía en hogares y fábricas y lo informan de forma intermitente, como un reloj, a la principal empresa de control.

Por lo tanto, la red inteligente, integrada en la computación de niebla se transformará en un marco estructurado de muchas capas con el intercambio entre el SCADA y la niebla. En dicho marco, una niebla es responsable de una rejilla miniaturizada e interactúa con las nieblas cercanas y en niveles más altos. Cuanto más alta es la capa, mayor es la latencia y más extenso es el alcance geofísico [6].

### 3.8. INDUSTRIA 4.0 Y SU RELACIÓN

Con la cuarta revolución industrial y el internet de las cosas, cada día se generan cientos de nuevos dispositivos conectados a internet, esto crece tanto en la sociedad

como en las industrias, por lo que un mejor control y manejo de datos es necesario, en este sentido la computación en la niebla es una solución práctica a este problema.

A partir de la digitalización de la industria, esta se expande a diferentes sectores, los cuales buscan facilitar y optimizar el uso de los diferentes dispositivos que conforman los sistemas, por ejemplo; una casa inteligente viene siendo integrada por diferentes dispositivos como calefacción, chimenea, horno o refrigerador. Los cuales son conectados a internet para conocer y controlar su funcionamiento desde casi cualquier lugar. Con este mismo principio se está buscando la creación de ciudades, automóviles y fábricas inteligentes [6].

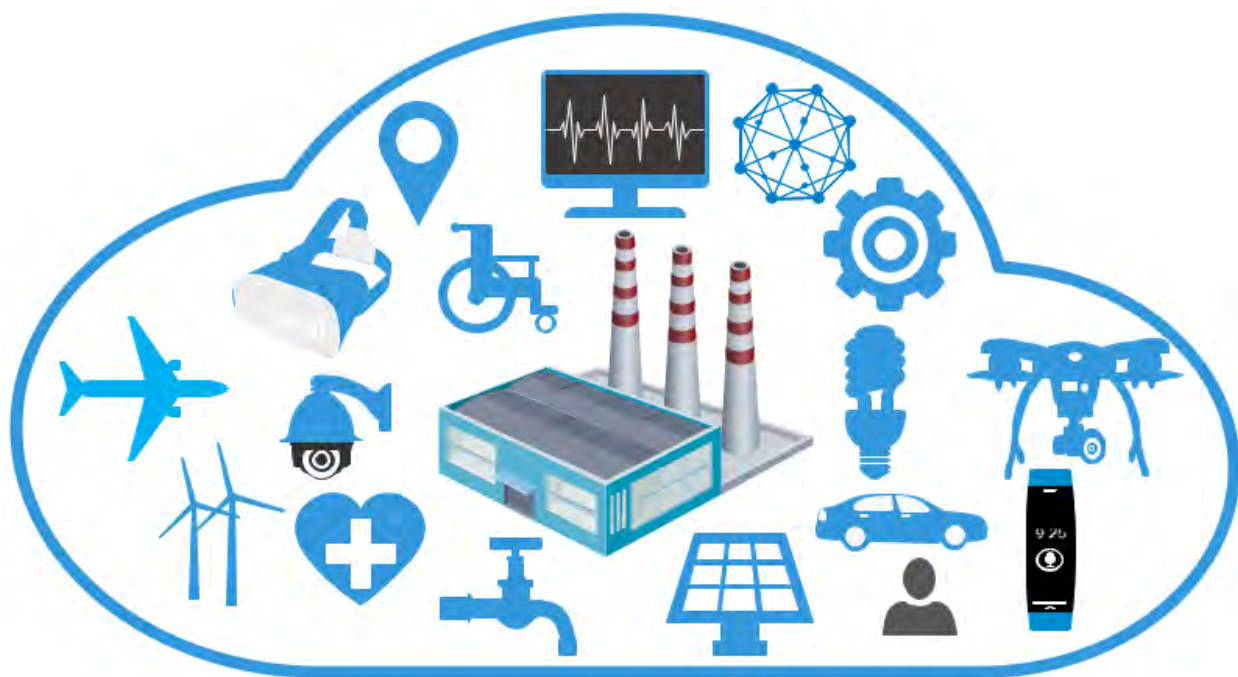


Ilustración 14.- Industria 4.0

### 3.9. AMBIENTE INTELIGENTE

Los escenarios y entornos inteligentes, como el hogar inteligente, la ciudad inteligente, dependen principalmente de la computación en la nube para su funcionamiento. Los servidores en la nube facilitan los objetos inteligentes para trabajar en conjunto y para correlacionar y cooperar. La característica prominente de los objetos inteligentes, sin embargo, es que están universalmente dispersos [6].



## CAPITULO 4. CLOUD, EDGE, IOT AND IOE

### 4.1. COMPUTACIÓN EN LA NUBE

Es una herramienta que permite el almacenamiento de datos en grandes cantidades, esto es de gran ayuda en las industrias y el internet de las cosas, ya que cada electrodoméstico, maquina o sensor genera datos de manera continua por lo que es necesario un lugar para almacenar y procesar dichos datos.

Todo esto es posible mediante el uso de dispositivos como; redes, servidores, almacenamiento, aplicaciones y servicios.

Una desventaja de esta herramienta, es que, al manejar grandes cantidades de datos, este servicio se puede ver afectado en el desempeño, viéndose reflejado en el tiempo de latencia.

Este paradigma cuenta con diferentes características que se muestran en la Ilustración 15, según la NIST [10]:

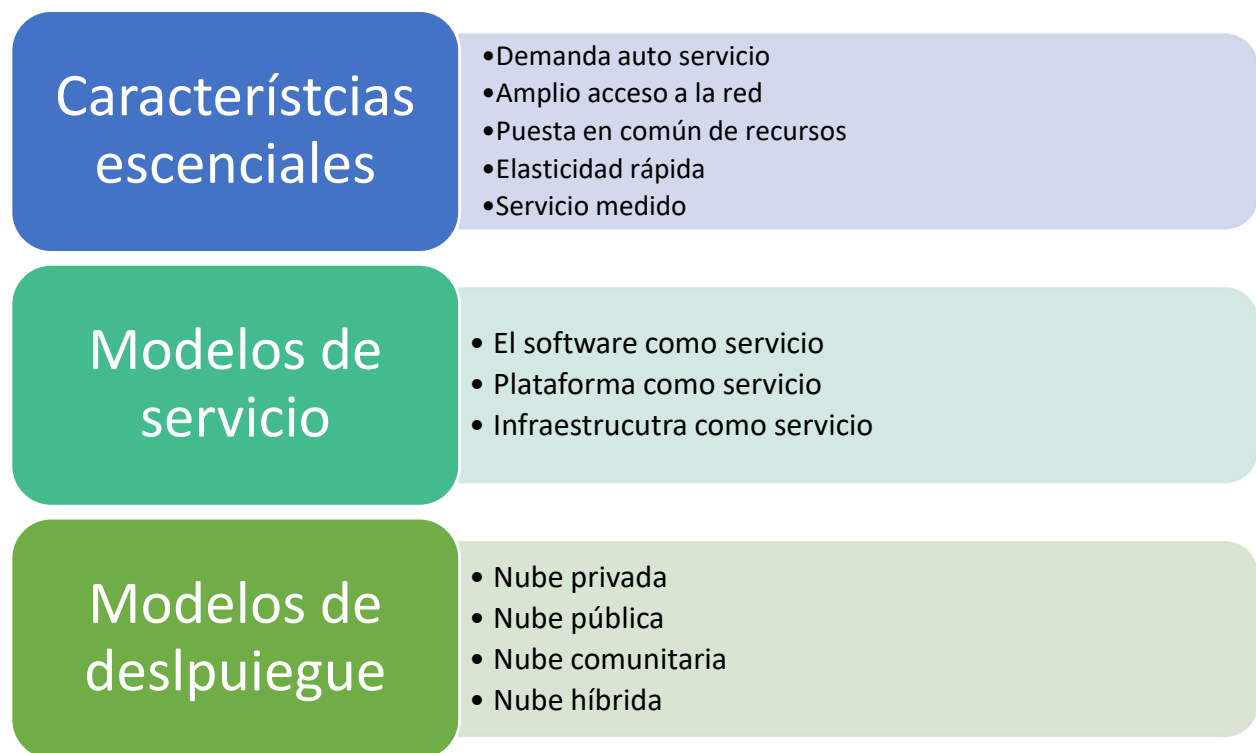


Ilustración 15 Características del cloud computing

## 4.2. COMPUTACIÓN EN LA NIEBLA VS COMPUTACIÓN EN LA NUBE

Para conocer las principales ventajas y desventajas para la computación en la niebla y en la nube, hay que conocer sus principales funciones para las que están diseñadas, la nube está hecha para manejar grandes cantidades de datos, sus centros de almacenamiento se encuentran en grandes centros de datos, los cuales tienen grandes centros de seguridad, y son administradas por grandes compañías generando un alto consumo energético. En cambio, la computación en la niebla propone que este servicio se encuentre más cercano a los usuarios, por lo que toda la arquitectura se encontraría en el lugar del servicio, teniendo como ventajas un menor consumo energético, una latencia menor entre otras, pero al estar cerca de los usuarios puede ser susceptible a ataques, estos ataques pueden ser perpetrados desde los diferentes dispositivos que comprende la red por lo que la seguridad se debe de llevar a ese nivel.

En comparación ambos servicios tienen una finalidad, la cual llega a tener ventajas y desventajas dependiendo el uso que se le quiera dar, por lo que no se puede definir una mejor que otra, aunque potencialmente la computación en la niebla tendrá un mayor uso por el surgimiento del internet de las cosas, para brindar un mejor servicio local y aliviar la carga de la nube [2], [3].

## 4.3. COMUNICACIÓN ENTRE LA COMPUTACIÓN EN LA NIEBLA Y EN LA NUBE

Como se podría entender geográficamente, la niebla es una extensión de la nube más cercana a la tierra, en este caso los aparatos, en este sentido la nube controla los servidores de la niebla, de esta manera la niebla solo puede controlar las aplicaciones que tenga cargadas a comparación de la nube que puede gestionar todo el contenido del sistema.

Un aspecto importante en la niebla es que esta puede compartir los datos más relevantes generados, de esta manera evita la saturación de la red ofreciendo un servicio rápido y eficiente a los que necesiten velocidad y baja latencia.

A continuación se muestra una tabla, en la cual se hace una comparación entre la computación en la nube y en la niebla [2]:

Tabla 2.- objetivos computacion en la niebla y computación de nube

Objetivo	Computación en la niebla	Computación en la nube
<b>Tipo de servicio</b>	Servicio de información limitado relacionado con ubicaciones de implementación específica	Información recolectada por todo el mundo
<b>Hardware</b>	Almacenamiento limitado, poder de cómputo e interfaz inalámbrica	Espacio de almacenamiento amplio y escalable, poder de cómputo
<b>Distancia a usuarios</b>	Próxima físicamente a través de una conexión inalámbrica	Muy lejana a los usuarios y comunicada a través de una res IP
<b>Ambiente de trabajo</b>	Fuera y dentro de edificios	Almacenes de gran tamaño equipados con sistemas de enfriamiento
<b>Despliegue</b>	Centralizado o distribuido en áreas regionales como lugares concurridos	Centralizado y mantenido por empresas grandes de internet
<b>Usuario objetivo</b>	Usuarios móviles	Usuarios de internet

#### 4.4. COMPUTACIÓN EN EL BORDE Y COMPUTACIÓN EN LA NIEBLA

Al igual que la computación en la niebla, la computación en el borde o Edge computing es un nuevo paradigma que busca hacer frente al internet de las cosas, ambos conceptos buscan acercar la nube a los usuarios, el borde es donde ocurren las conexiones, esta conectividad se puede dar alámbrica o inalámbrica para el manejo de datos de forma local, debido a la cercanía de los dispositivos, estos datos son manejados en tiempo real, esta es una ventaja para los diferentes sistemas dinámicos que necesitan tiempos de respuesta corto.

A continuación, se muestra una tabla comparativa de la computación en el borde y en la niebla.[11]

*Tabla 3 Computación en la niebla vs computación en el borde*

	<b>Computación en el borde</b>	<b>Computación en la niebla</b>
<b>Arquitectura</b>	Jerárquica, descentralizada y distribuida	Jerárquica, descentralizada y distribuida
<b>Proximidad a los dispositivos</b>	Localizada en los dispositivos	Cerca de los dispositivos
<b>Latencia</b>	baja	Baja
<b>Costo de banda</b>	Baja	baja
<b>Recursos</b>	Más limitada	Limitada
<b>Computación y capacidad de almacenamiento</b>	Más limitada	Limitada
<b>movilidad</b>	Soporte	Soporte
<b>Escalabilidad</b>	Alta	alta
<b>Servicio</b>	virtualizado	virtualizado
<b>Ubicación de datos, procesamiento, colección, tratamiento y almacenamiento</b>	Dispositivos del borde y redes del borde	Cercano al borde y núcleo de red, dispositivos en el borde y núcleo de la red.
<b>Manejo de aplicaciones para el internet de las cosas</b>	Sin soporte	Con soporte
<b>Enfoque</b>	Nivel de las cosas	Nivel infraestructura

#### 4.5. INTERNET DE LAS COSAS Y LA COMPUTACIÓN EN LA NIEBLA

La cuarta revolución industrial es un hecho hoy en día, ya que cada vez podemos estar más conectados a internet, y no solamente desde nuestros dispositivos móviles, sino también nuestros aparatos electrónicos, vehículos o sensores. Estos aparatos generan una gran cantidad de información, la cual es almacenada en la nube, con el creciente número de datos de estos aparatos que cada vez se conectan a internet dentro de unos años la nube no será suficiente para almacenar y procesar toda esa información. Por esto la computación en la niebla se propone como una solución a el internet de las cosas [6].

#### 4.6. RETOS PARA LA COMPUTACIÓN EN LA NIEBLA

Con los nuevos avances tecnológicos, la computación en la niebla se ve forzada a superar nuevos retos para cumplir con los requerimientos del cliente y las nuevas tecnologías, estos retos que expone M.Chiang and L Chang [35] se muestran en la Tabla 4.

Tabla 4 Retos para la Computación en la Niebla

Retos para el internet de las cosas		Como la computación en la niebla los puede resolver
<b>Restricciones de latencia</b>	<b>de</b>	Se busca que la computación en la niebla realice todas las operaciones de cálculos, gestión y el análisis de datos, así como otras funciones sensibles al tiempo cerca de los usuarios finales, de dicha manera se satisfacen los requisitos de latencia
<b>Restricción de ancho de banda</b>		La computación en la niebla permite el procesamiento jerárquico de datos a lo largo de la nube para dispositivos IoT. Esto permite que el procesamiento de datos se lleve a cabo dependiendo de las demandas de la aplicación, redes y recursos informáticos disponibles. Esto, a su vez, reduce la cantidad de datos que deben cargarse en la nube, lo que ahorrará el ancho de banda de la red.

<b>Recursos limitados en dispositivos</b>	La computación en la niebla puede ser usada para operaciones que necesiten gran cantidad de recursos, a causa de dispositivos de los cuales sus operaciones no pueden ser subidas a la nube, por lo tanto, esto permite reducir la complejidad de los dispositivos, los costos del ciclo de vida y el consumo de energía.
<b>Servicio ininterrumpido</b>	La computación en la niebla puede ejecutarse de forma independiente a la nube, incluso cuando la conectividad es irregular, todo para garantizar un servicio continuo.
<b>Seguridad para el internet de las cosas</b>	Los dispositivos con recursos limitados tienen funciones de seguridad limitadas; por lo tanto, la computación con niebla actúa como el pro para que estos dispositivos actualicen el software de estos dispositivos y la seguridad

#### 4.7. NIEBLA EN IOT Y CLOUD OF THINGS

Con el surgimiento del internet de las cosas el manejo de información se ha dificultado por la gran cantidad de datos que se generan de manera continua, por tanto, se ha buscado la unión del internet de las cosas con la nube, por lo que se le llamó *Cloud of things* o en otras palabras la nube de las cosas, teniendo como función alimentar y ayudar al desarrollo de contenido de medios e información.

Muchos servicios del internet de las cosas exigen soluciones rápidas y precisas, como lo pueden ser servicios sanitarios de hospitales y situaciones de crisis exigen respuestas rápidas y en tiempo real, en este sentido no toda esta información generada puede ser clasificada para ser enviada a la nube para evitar una sobrecarga de la transmisión, por lo tanto, se ha confiado en la computación en la nube para el desarrollo de estas tareas y trabajar como mediador entre el IoT y la nube [6].

Su actividad principal es supervisar los activos, el pre-procesamiento, la filtración de información y los esfuerzos de seguridad. Por esta razón, Fog necesita un sistema de administración de activos exitoso y efectivo para IoT. Una utilización distintiva de la computación de niebla se encuentra en la Internet Industrial de las Cosas (IIoT). Aquí, las

máquinas y diferentes sensores, pasarelas y actuadores integrados en un sitio web de producción pueden utilizarse como sistema de niebla para ampliar la productividad [36].

#### 4.8. INTERNET OF EVERYTHING

Internet of Everything (IoE) es una interconexión de individuales, datos, métodos y dispositivos. Identifica la convergencia de numerosos entornos, como la computación en la nube, la movilidad, el procesamiento de datos y, para terminar, una explosión en cosas interconectadas. El IoE integra las diversas metodologías y técnicas, trata de construir un mecanismo de proceso e incluye individuos en este método para desarrollar sistemas inteligentes adicionales [5].

El IoE integra las diversas metodologías y técnicas, intenta construir un mecanismo de proceso, e incluye métodos individuales para desarrollar sistemas inteligentes adicionales. IoE se utiliza principalmente para recopilar y examinar información de diversas fuentes, como instrumentos, dispositivos de sensores, equipos de procesamiento de pagos, dispositivos móviles, almacenes de datos, y también se utiliza para encontrar predicciones en el futuro. El IoE está creando nuevos desafíos y oportunidades que se analizarán durante los años siguientes. Se producirán y consumirán grandes cantidades de datos, por lo que los marcos de Internet de las cosas necesitarán identificar nuevas metodologías y técnicas asociadas al análisis, el rendimiento y la escalabilidad de big data. Consideramos que la configuración de nubes locales de dispositivos, cerca de la ubicación donde se producen y consumen los datos, es una buena solución para resolver estos problemas que también pueden involucrar en la seguridad [5].

En general, las conexiones a Internet siempre se usan para la computadora portátil, las computadoras de escritorio y las tabletas. Hoy en día, muchos dispositivos avanzados, como el reloj de presión cardíaca, el cinturón de temperatura corporal, etc., también están conectados a Internet para transferir continuamente la información de salud del individuo no solo en la atención médica, sino también en más aplicaciones como ciudad inteligente, control de tráfico inteligente y aplicaciones de monitoreo del clima. Normalmente, las tecnologías IoE varían en el rango de dispositivos sensores digitales utilizados para diversas aplicaciones a dispositivos inalámbricos

interconectados más inteligentes y numerosos, aplicaciones industriales inteligentes y diversas tecnologías de hardware distribuido que se han vuelto más automatizados e inteligentes. El trabajo de Mavromoustakis et al. [6] propone un esquema para compartir recursos utilizando el paradigma de redes oportunistas, mientras que habilita la EC al asignar horarios diferentes de reposo / vigilia basados en tráfico en tiempo real a dispositivos inalámbricos. El esquema considera el intercambio de recursos de proceso, que, de acuerdo con la duración del tráfico a través del canal asociado, afecta la duración del tiempo de inactividad del nodo [5].

Recientemente, el término loE juega un papel vital en los campos de la tecnología de la información. Por ejemplo, Cisco es uno de los institutos líderes que se ha centrado más en tecnologías basadas en loE. loE se ha mejorado de las versiones anteriores de tecnologías basadas en Internet como IoT, Internet de humanos, IoT industrial e Internet de digital. En otras palabras, loE es un sistema con conectividad de extremo a extremo entre procesos, tecnologías y conceptos involucrados en todos los casos de uso de conectividad. loE consiste básicamente en cuatro partes de conexión, como personas, cosas, datos y procesos [5].

#### 4.8.1. PERSONAS

Los nodos de destino o destino están interconectados con Internet para distribuir actividades y datos. loE permite a las personas conectarse a Internet de maneras incalculables. Hoy en día, muchas personas se conectan a Internet utilizando sus propios dispositivos inteligentes, como PC, televisores, tabletas y teléfonos inteligentes. Además, también usan redes sociales como Twitter, Facebook, LinkedIn y Pinterest. A medida que Internet crezca hacia loE, estaremos conectados de maneras más relacionadas y útiles [5].

#### 4.8.2. COSAS

Las cosas son el componente más importante en el loE utilizado para observar los datos más relevantes de los dispositivos físicos. Los datos recopilados de dispositivos loE se utilizan para tomar decisiones valiosas en situaciones de emergencia y de futuro cercano. Por ejemplo, los dispositivos médicos inteligentes en la aplicación de atención



médica loE se utilizan para observar la información de las personas que monitorea eficientemente la salud del paciente en caso de emergencia. Esta información recopilada se transfiere al almacén de datos para analizar otras decisiones apropiadas y valiosas [5].

#### 4.8.3. DATOS

Los dispositivos IoT normalmente recopilan datos y los transmiten a través de Internet a un servidor de sensores, donde se procesan y analizan. Debido al hecho de que las capacidades de las cosas conectadas a Internet persisten para avanzar, se volverán además intelectuales al combinar datos en información más valiosa. Los datos no procesados después de ser generados desde los dispositivos serán procesados y analizados en estadísticas valiosas para proporcionar mecanismos de control y decisiones inteligentes. Por ejemplo, las mediciones de frecuencia cardíaca alta y baja se utilizan para encontrar la frecuencia cardíaca promedio del paciente en la industria de la salud [5].

#### 4.8.4. PROCESOS

El proceso desempeña un papel importante en la medición de cómo entidades como datos, personas y cosas trabajan con otros para aportar valor al mundo conectado de loE. Con el proceso preciso, las conexiones se convierten en aplicables y agregan valor porque la información exacta se transfiere al destino o dispositivo específico de la manera adecuada. Además, la sólida conectividad entre los dispositivos inteligentes, los datos y las personas se utiliza para obtener información valiosa del sistema loE. Por ejemplo, el uso de redes sociales y dispositivos inteligentes de acondicionamiento físico para promover ofertas de atención médica pertinentes a posibles clientes [5].

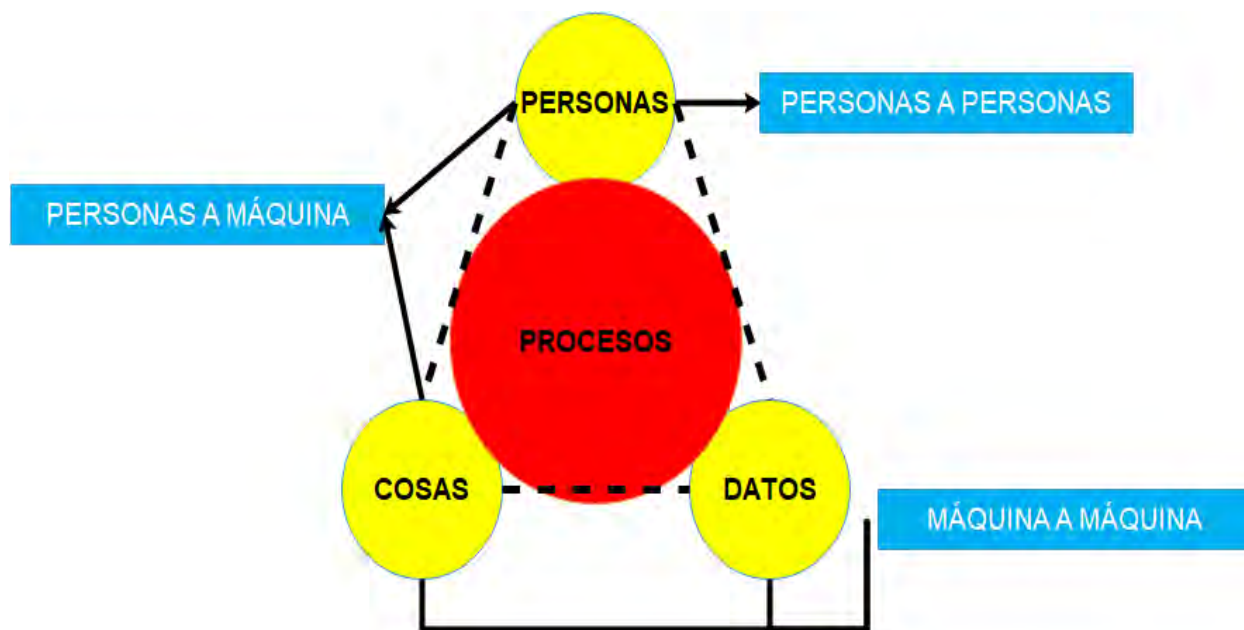


Ilustración 16.- Personas, cosas, datos y procesos de IoT

#### 4.9. USOS PARA LA PRÓXIMA GENERACIÓN

Los servicios ofrecidos por IoT permiten desarrollar varias aplicaciones de diferentes industrias que actualmente sufren muchos atributos como costo, mantenimiento, recursos, etc. En los próximos días, habrá aplicaciones actuales con inteligencia para convertirlas en una industria de telecomunicaciones inteligente, una industria médica y de salud inteligente, una vida independiente inteligente, una industria farmacéutica inteligente, una industria minorista inteligente y sistemas logísticos inteligentes. Las siguientes son las diferentes industrias: industria aeroespacial y de aviación, industria automotriz, industria de telecomunicaciones, industria médica y de atención médica, vida independiente, industria farmacéutica, comercio minorista, logística, gestión de la cadena de suministro, transporte, agricultura e industria manufacturera que buscan utilizar IoT tipo de término tecnológico para hacer que nuestra próxima generación sea más inteligente. [5]

En la aplicación de atención médica inteligente, los centros y laboratorios de clínicas médicas están pasando de proporcionar pruebas y diagnósticos de los pacientes en las instalaciones, es decir, en hospitales y clínicas, para aislar el autocontrol. El autocontrol beneficia a los pacientes al proporcionarles una mayor libertad e

individualidad para observar el estado de salud del paciente. Conducirá a mantener al paciente en casa o en qué lugar necesitaba apoyarse y alentarse a sí mismo, que se siente asustado por la atmósfera del hospital [5].

Para la aplicación de logística inteligente basada en IoT, es posible visualizar que los bienes o productos pueden transportarse sin la participación de recursos humanos en ciertas áreas, desde compañías hasta comerciantes. Este sistema hace que los almacenes estén completamente programados para tomar decisiones inteligentes con la entrada y salida de mercancías, según las estadísticas recibidas a través de dispositivos y sistemas de posicionamiento global (GPS) para minimizar las direcciones de tránsito [5].

## CAPITULO 5. SEGURIDAD

Los dispositivos y dispositivos informáticos de niebla pueden enfrentar problemas de seguridad genuinos del marco, ya que los dispositivos de niebla se usan normalmente en lugares que están fuera del ámbito de la protección y la observación. Posteriormente, terminan expuestos a agresiones maliciosas, como la incautación y escucha de información que puede poner en peligro el funcionamiento y los sistemas de los dispositivos de niebla. La computación en la nube es afortunadamente una miríada de soluciones, que podrían no ser efectivas en el caso de la computación de niebla, ya que los dispositivos y dispositivos que dependen de la computación de niebla operan al borde de la red [1].

### 5.1. PROBLEMAS ABIERTOS

Los dispositivos que usa la computación en la niebla para su funcionamiento pueden enfrentar graves ataques a los sistemas de seguridad, esto debido a que se encuentran en lugares sin una estricta protección y vigilancia, por lo que pueden ser intervenidos [1].

Los problemas que enfrenta la computación en la niebla no pueden ser prevenidos como los que presenta la computación en la nube, por lo tanto, existe vulnerabilidad como los problemas que se describe a continuación [1]:

#### 5.1.1. HOMBRE A LA MITAD

Este puede llegar a ser el problema más común, y consiste en que un intruso pueda ver o interrumpir los paquetes entre dispositivos de niebla, debido a que estos no cuentan con protocolos de comunicación seguros por la falta de recursos, este problema no tiene una solución definida [30], [6].

#### 5.1.2. DISTRIBUCIÓN DENEGADA DEL SERVICIO

Esta es conocida como la amenazada de seguridad más desafiante para los sitios WEB y servicios en línea para la actualidad, los nodos de niebla son recursos restringidos, por lo que es difícil lidiar con un gran número de solicitudes

simultáneamente. Mediante el lanzamiento de una gran cantidad de servicios irrelevantes, lo que ocuparía a los nodos durante un largo periodo de tiempo, por lo que se vería afectado este servicio, de igual manera los nodos de niebla pueden ser usados para lanzar este tipo de ataques [32].

### 5.1.3. TOLERANCIA A ERRORES

Para que la computación en la niebla brinde un servicio de calidad debe estar preparada para responder al presentarse fallos en el sistema, en este sentido se tiene una ventaja ya que es un sistema descentralizado, por lo que, al fallar un componente, los dispositivos se pueden conectar a el más cercano posible sin presentar mayores problemas.

## 5.2. CONFIANZA.

La confianza asume una parte notable en el fomento de las relaciones a la luz de las asociaciones pasadas entre nodos de niebla y dispositivos de borde. Un nodo de niebla es considerado como la parte más importante ya que es responsable de garantizar la seguridad y la anonimidad de los clientes finales. Además, se debe confiar en esta parte para llevar a cabo su tarea, ya que se debe garantizar que el nodo de niebla actualiza el proceso de cobertura mundial en su información descargada y desencadena solo acciones no amenazadoras. Esto requiere un cierto grado de confianza entre todos los nodos que operan dentro de la red de niebla [33], [1].

### 5.2.1. ENGAÑO DE COLUSIÓN

El sistema de suscripción pública ha sido usado en diferentes sistemas cruciales como el monitoreo y verificación de tráfico a gran escala, este mismo sistema puede ser usado para la computación en la niebla, empleándola para separar la interacción de los usuarios y ofrecer comunicaciones que no están sincronizadas [34].

Un nodo de suscriptor o publicador maligno que esté programado para retener el contenido de datos de otros nodos o la clave de cifrado oculta lanzará intencionalmente a los corredores opuestos la clave hasta ahora oculta [11].

En su estudio, Wang et al. contempla el plan de confianza en la computación de niebla que incorpora lo que se llama un sistema de suscripción pública (PSS), para salvaguardar la confianza contra ataques de colusión concertados. En varios sistemas grandes como el monitoreo y la verificación del tráfico, el PSS generalmente se ha utilizado a gran escala. Aquí, se presenta un protocolo de PSS basado en un agente no específico, que muestra la parte de un agente como parte esencial de un PSS.

Los corredores realizan su trabajo interactuando con editores y suscriptores, y armonizando las demandas apropiadas de los usuarios y luego transfiriendo la información de los usuarios. Ellos pueden ser empleados para separar la interacción de los usuarios y ofrecer comunicaciones que no están sincronizadas. Un nodo de suscriptor o editor maligno que está programado para retener el contenido de datos o el cifrado de otros nodos. La clave oculta liberaría intencionalmente a los corredores opuestos la clave oculta hasta ahora. A continuación, se enumeran las formas en que los nodos y corredores malignos pueden conspirar entre sí y divulgar secretos:

1. Un nodo maligno ofrece información crucial de otros usuarios a un agente nocivo que evalúa esta información.
2. El agente maligno ofrece información de otros nodos a sus colisionadores, para engañar a otros usuarios haciéndoles creer que los colisionadores son la entidad apropiada.

Por lo tanto, se puede inferir que los corredores pueden ser nocivos y la niebla enfrenta asaltos intrigantes. Para disminuir los peligros y vulnerabilidades de seguridad, la prueba sugiere contenido relacionado PSS con protección variable en una configuración de niebla que garantizaría el funcionamiento confiable y la entrega de publicación y suscripción [1].

### 5.2.2. SEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

Los dispositivos que usan nodos de niebla, al estar cerca de los usuarios finales, se llevan a lugares que pueden no ser tan seguros. Tales dispositivos podrían volverse vulnerables a ataques viciosos injustificados. Por ejemplo, en el ataque Man-in-the-

middle, esencialmente es una estrategia de secuestro de datos, los dispositivos de nodo de niebla podrían cambiar virtualmente a ser falsos. Este problema, sin embargo, podría tratarse efectivamente con los enfoques de descifrado y cifrado. Otro tema delicado es la integridad y confidencialidad de los datos. Este problema surge porque en la computación de niebla, una plataforma ampliamente dispersa, los dispositivos en el borde crean enormes volúmenes de datos que, por cierto, tienen que ser transmitidos a los nodos de niebla para almacenar y guardar, así como para la computación. Además, los nodos de niebla a menudo tienen que interactuar con gadgets de borde y conjuntos de datos en la computación en la nube. Todas estas operaciones complejas hacen que los datos sean vulnerables a la exposición y al pirateo. Sin embargo, una solución para abordar este problema es simplemente emplear técnicas de enmascaramiento o algoritmos de encriptación ligeros. Además, en la computación en niebla hay una gran cantidad de áreas donde se lleva a cabo la colaboración, esto puede dar lugar a problemas relacionados con la privacidad y la seguridad. Estas áreas problemáticas incluyen autenticación, autorización, administración de identidades, control de acceso a los recursos, aplicación y decisiones distribuidas de manera segura, calidad de seguridad y servicio, intercambio de políticas de información [1].

### 5.2.3. CONFIANZA EN MIDDLEWARE Y SPECIMEN

En su trabajo, Elmisery et al. presentó un middleware basado en la niebla, en el que los operadores de confianza calculan la confianza relacional estimada entre la nube y un nodo de niebla. Se realiza el cálculo de la confianza de manera descentralizada mediante el uso de la definición de entropía. Para obtener privacidad para el usuario, el operador de cobertura cercano ejecuta el procedimiento de camuflaje del vecindario. El operador de cobertura mundial, que solo existe en un nodo de niebla, realiza el proceso de disfraz mundial en el perfil del cliente recopilado. Para mejorar y controlar la confianza, una administración y servicio el nivel está incorporado en la estructura de niebla [1].

En su estudio, Soleymani et al. indican que, para garantizar la fiabilidad e integridad de las aplicaciones, es crucial establecer la confianza entre los vehículos. En situaciones vehiculares, un paradigma de confianza protegido es capaz de gestionar vulnerabilidades y asumir riesgos, derivados de datos no confiables. Pero se encuentra

que los automóviles y otros vehículos a menudo acumulan, además de obstáculos ambulatorios y no ambulatorios, datos que simplemente son incorrectos, deficientes, inciertos y llenos de errores [1].

Por lo tanto, para engendrar una red vehicular segura, se propone un paradigma de confianza difusa consolidado en participación, experiencia y credibilidad. Realiza una progresión de controles de seguridad para garantizar la precisión de los datos obtenidos de vehículos aprobados. Además, los nodos de niebla están afiliados como un instrumento para evaluar el grado de precisión del área de una ocasión o evento [1].

En este contexto, Koo et al. ha presentado un paradigma de seguridad mixta que elimina la duplicación al considerar escenarios falsos de ahorro y reserva de niebla. Para salvaguardar la privacidad, este trabajo interpone un tercero de confianza (TPP) en la operación. Los ataques nocivos pueden hacer que los intercambios de sensores sean engañosos y cuestionables. Por eso, una técnica de evaluación de confianza es imprescindible para garantizar una relación de calidad inquebrantable entre los sensores para oponerse a los ataques nocivos. Los nodos de niebla se incorporan para permitir que el marco descifre los valores de confianza [1].

#### 5.2.4. CONFIANZA BASADA EN EL ÁREA

En la niebla, existen varios dispositivos físicos en diversas áreas que tienen diferentes tipos de comunicación y estructuras de redes. Aun así, para ofrecer reacciones más rápidas, los nodos de niebla están equipados para ofrecer ambos: servicios de computación regionales y locales. Entonces, la cuestión de cómo lograr estos objetivos en concierto con los atributos de la niebla forma un área de estudio para el futuro. Para efectuar la interacción basada en la confianza y la comunicación entre los nodos de niebla en lugares ampliamente difundidos, Dang et al. han avanzado un paradigma de confianza basado en áreas [1].

En este escenario, se elige un nodo de niebla para designar la administración de activos computacionales y la ejecución de trabajos en un entorno local. Por ejemplo, si



el nodo 2 en el área A y el nodo 4 en el área B se eligen como designados por separado, los nodos designados se utilizan para calcular estimaciones de confianza o valores para nodos en un área similar. Entonces, por ejemplo, si el nodo 1 necesita obtener la estimación de confianza del nodo 3, necesita adquirirlo por medio del nodo 2 en la región A. Y si el nodo 1 desea asegurar el valor de confianza del nodo 5, es necesario que páselo por el nodo 4 en el área B. Al mismo tiempo, también pueden averiguar su confianza de área, estimaciones y transmitir las a la nube [1].

### 5.3. PENETRACIÓN

Los dispositivos y dispositivos con nodos de niebla se llevan a todo tipo de lugares, incluidos aquellos donde la protección es débil o ausente. Por lo tanto, pueden enfrentar penetraciones maliciosas. Además, un cliente nocivo puede registrar lecturas incorrectas o falsas, falsificar ubicaciones y direcciones IP o alterar su propio medidor inteligente [1].

#### 5.3.1. NODOS MALICIOSOS Y SUS PENETRACIONES

*Penetraciones de nodos maliciosos de niebla:* Lee et al. han analizado las partes y las amenazas singulares contra la seguridad de IoT en la niebla. Como uno de los peligros potenciales, la preocupación de un nodo de niebla malicioso está lejos de ser trivial, su estudio muestra que los nodos de niebla procesan en la niebla la carga de trabajo densa que se segmenta en diferentes tareas. En su exploración, las cargas de trabajo sustanciales en la niebla se separan en algunas ocupaciones y se preparan mediante nodos de niebla. En el caso de que una parte de estos nodos sea atacada por clientes maliciosos, es difícil garantizar la seguridad de la información. Sin embargo, los autores no presentaron una solución sobre cómo ocuparse de tal penetración. Por otro lado, Z. Li, X. Zhou et al. estudiaron el crecimiento de ganglios maliciosos en la niebla. Primero investigaron, como interactuaban los nodos maliciosos y los nodos susceptibles. Luego evaluaron, analizaron y descubrieron el proceso de toma de decisiones.

*Asaltos por mecanismos de borde maliciosos de clientes:* para la protección de la información en la niebla, es crucial identificar los dispositivos y dispositivos de borde que se han vuelto maliciosos. Aun así, es difícil evitar la penetración en vista de los beneficios específicos que se les conceden para utilizar y procesar la información. En este contexto,

Sohal et al. sugirió una estructura mediante el uso de un modelo de Markov, un marco de identificación de interrupciones y un dispositivo virtual honeypot para solucionar el problema [1].

### 5.3.2. PENETRACIÓN MITM

Todo el tráfico y la interacción entre los nodos de niebla y los dispositivos y dispositivos de borde están protegidos por canales de transferencia seguros y protegidos. Aun así, un atacante externo puede espiar o cambiar la información descargada de un cliente antes de que el nodo de niebla ejecute un proceso de ocultación mundial. MITM es un tipo de penetración tan frecuente. El atacante externo perturba efectivamente el canal OpenFlow y controla la entrada después de ejecutar los cuatro artificios mencionados a continuación [1]:

- 1.-Para un dispositivo dentro de la LAN de IoT, el atacante externo puede usurpar el control propulsando un ataque de actualización de firmware, ya que los dispositivos inteligentes integrados son indefensos frente a los ataques.

- 2.-El dispositivo inteligente luego inyecta un respaldo del cliente en el nodo de niebla, afirmando falsamente que el nodo de niebla tiene que utilizar este adjudicación para revelar su identidad en intercambios posteriores.

- 3.-Después de que el nodo de niebla implanta el certificado del cliente, el atacante externo corta la asociación entre este y el controlador.

- 4.-Finalmente, el atacante ejecuta la penetración MITM en el canal de control OpenFlow.

En su investigación, C. Li, Z. Qin et al. han discutido la preocupación de seguridad de un canal OpenFlow entre el controlador y sus operadores en la niebla de IoT. Dado que todos los cargos del controlador se envían a través de este canal, una vez penetrado, el sistema es totalmente manipulado por un atacante. En este contexto, I. Stojmenovic

et al. propusieron utilizar el filtro Bloom para reconocer el asalto MITM. En su estudio, Stojmenovic et al. investigaron el ataque de MITM y sus características secretas a través de la investigación del consumo de memoria y la CPU del dispositivo de niebla.

#### 5.4. CONTROL DE ACCESO

Este más que una amenaza hay que plantear como se cumplirán los objetivos y restricciones a diferentes niveles en esta relación que va desde el usuario, la computación en la niebla para finalmente llegar a la nube. Esto se puede llevar a cabo mediante sistemas de cifrado y buscar que se garantice la seguridad en el sistema [1].

##### 5.4.1. CIFRADO DE CALIDAD

La niebla evoluciona y es una expansión significativa de la computación en la nube. Por lo tanto, es natural que adquiera numerosas dificultades de seguridad relacionadas con la privacidad de la computación en la nube. Pero muchas de las soluciones habituales de la computación en la nube son útiles en la computación en niebla. Por ejemplo, se pueden emplear los cálculos, Rivest Shamir Adleman y Advanced Encryption Standard, las soluciones de encriptación normalmente preferidas. [1]

En su trabajo, Fan et al. Han llamado la atención sobre el hecho de que, para obtener el control del acceso a los datos en las plataformas de nube y niebla, el cifrado basado en atributos de contenido de cifrado (ABE) puede ser útil. En consecuencia, proponen un plan de control de entrada basado en múltiples autoridades subcontratadas que se puede verificar. La criptografía basada en atributos funciona como una innovación sobresaliente para garantizar el secreto de la información y controlar el ingreso a la información ajustada. El trabajo propone un plan seguro para el control del acceso a datos optimizados combinado con la externalización de cómputo y la actualización de texto cifrado para IoT en cómputo de niebla. Puede disminuir el costo de la computación y garantizar un control seguro del acceso a la información [1].

El marco comprende servidores en la nube, características principales, nodos de niebla y clientes. Para cada nodo de niebla y servidor, el atributo principal genera una clave pública. También produce una clave oculta para cada dispositivo y dispositivo en el borde de los clientes. La información de comunicación se presenta en contenido

cifrado para niebla a niebla y niebla a nube, mientras que es contenido cifrado limitado para borde a niebla [1].

Los medidores inteligentes pueden codificar y enviar la información a un dispositivo de niebla, como, por ejemplo, un gateway de la red de área local, luego ensamblar los resultados y finalmente transmitirlos a la nube, si es necesario. Aquí, Jiang et al. llaman la atención sobre el hecho de que algunas circunstancias molestas y la infracción de un enfoque de control de entrada pueden aparecer con el argumento de que un cliente puede producir otra clave privada para el derecho de entrada. Para solucionar el problema, sugieren una técnica para determinar este problema formalizando las necesidades de seguridad y desarrollando un plan de cifrado basado en características (ABE) para cumplir con los nuevos requisitos previos de seguridad.

Para facilitar la comunicación personal y de buena fe entre un grupo de nodos de niebla, Alrawais et al. presentan un paradigma comercial clave formado en cifrado basado en características de política de texto cifrado (CP-ABE) para establecer intercambios seguros entre los miembros. Fusionaron la firma digital y los protocolos CP-ABE, para lograr la validación, privacidad, control de acceso e irrefutabilidad. Junto con un servidor que crea una clave, la estructura comprende segmentos como el servidor de creación de claves, la nube, los dispositivos de IoT y los nodos de niebla. El servidor de creación de claves se emplea para producir y distribuir las claves entre los segmentos incluidos. La nube caracteriza una estructura de entrada a todos los nodos de niebla y ejecuta el cifrado para obtener contenido de cifrado [1].

#### 5.4.2 PERFIL DE COMPORTAMIENTO

En su investigación, Mandlekar et al. llaman la atención sobre el hecho de que la entrada no autorizada debe ser identificada y la información genuina debe ser conservado sin ser atacado. Posteriormente, para hacer coincidir el comportamiento de un usuario con el de los usuarios regulares para la verificación, recurren a la tecnología de perfiles de comportamiento e información de señuelo [1].

## 5.5. COMUNICACIÓN SEGURA

En comunicaciones hay dos tipos:

- 1) Comunicaciones entre dispositivos o dispositivos de IoT restringidos y nodos de niebla.
- 2) Comunicaciones entre nodos de niebla.

Puede haber mensajes falsos durante la comunicación cuando los atacantes en la red envían datos falsos. Mukherjee et al. afirman que las características de seguridad deberían ser potentes y adaptables en un escenario de niebla restringido por activos mientras los datos se transmiten desde el borde a la nube. Para las interacciones y conversaciones de niebla a nube, esbozan un sistema de seguridad de extremo a extremo irregular y adaptable para las comunicaciones entre niebla y nube. Puede gestionar asociaciones problemáticas del sistema y lograr configuraciones de seguridad acordes con los diversos requisitos de la aplicación. En su trabajo, Wang et al. sugieren un plan para salvaguardar las identidades de los dispositivos periféricos mediante el uso de alias y para garantizar la ocultación de la información utilizando un método de cifrado similar mientras se transfiere información de los dispositivos periféricos a la nube [1].

## 5.6. PROTECCIÓN DE LA PRIVACIDAD

La protección de la privacidad es absolutamente esencial a la luz de las numerosas preocupaciones de los usuarios sobre su delicada información. Se presentan diversos enfoques, planes y técnicas de protección de la protección, particularmente en el área de la salud. A la luz de varios avances, a continuación, se describen ciertos trabajos relacionados [1].

### 5.6.1. ÁREA DE PROTECCIÓN DE LA PRIVACIDAD

En el área de niebla, las preocupaciones de privacidad siguen siendo una prueba. Con la ayuda de la niebla, los servicios basados en el área, que son favorecidos por muchos, pueden lograr baja latencia. J. Kang, R. Yu et al. en su estudio examinaron un protocolo de protección de la privacidad relacionado con áreas. En su trabajo, Kang et

al. insisten en las preocupaciones de privacidad del área relacionadas con el Internet de vehículos (IoV) respaldado por niebla que aspira a superar problemas como una enorme latencia y gastos alucinantes [1].

En consecuencia, se introduce un alias de protección de la privacidad para la gestión de *nom de plume* viable. El trabajo reconoce la protección direccional de la privacidad apoyada en la niebla para los servicios del área de la nube. El documento exhibe un plan redundante basado en un círculo de niebla para salvaguardar la privacidad del área del nodo fuente y lograr la capacidad de energía de niebla. El estudio sugiere una convención de criptografía posicionada para salvar la privacidad del área. Los nodos de niebla son particularmente capaces de satisfacer las necesidades de aplicaciones específicas del área y la administración de información consciente del área, como en las redes provisionales de vehículos [1].

#### 5.6.2. OTRA PROTECCIÓN DE PRIVACIDAD

En su trabajo, Du et al. señalan el problema de privacidad que está incorporado en una etapa de niebla y proponen un modelo de cuestionario basado en la privacidad diferencial. Wang et al. sugieren un plan de protección de la privacidad mediante la utilización de privacidad diferencial en la niebla, que al mismo tiempo puede garantizar la confidencialidad y privacidad de los clientes [1].

Por otro lado, R. Lu, K. Heung et al. señalan que la mayoría de los planes de conglomeración de información para ahorrar privacidad refuerzan la agregación de información solo para dispositivos IoT diversificados y no pueden combinar la información total de los dispositivos híbridos IoT en una sola unidad. En consecuencia, se avanza un plan total de información de ahorro de privacidad ligero para el IoT actualizado con niebla. En su estudio, Elmisery et al. examinan y descubren el límite de revelación entre publicidad y privacidad como también entre uno mismo y otros. Por otro lado, Hu et al. proponen un plan de protección de la privacidad para distinguir la cara utilizando la niebla. La red provisional vehicular empapada de niebla es otro protocolo que es beneficioso para la niebla y la nube vehicular, para lo cual se propone un plan de navegación seguro y privado [1].

## 5.7. OTROS

*Accesibilidad al servicio:* incorpora cómo disminuir la denegación de servicio (DOS). En el momento en que hay una gran cantidad de demandas de los clientes por el mismo servicio, DOS sucede si los piratas informáticos explotan la situación para atacar. Se sugiere buscar un nuevo plan para proteger los ataques de DOS. Deben pensarse en técnicas más nuevas para evitar la utilización innecesaria y el desperdicio de recursos y proporcionan capacidades de reserva adecuadas para mejorar la accesibilidad de los servicios.

*Aplicaciones seguras:* Mientras tanto, Khan et al. resumen las posibles preocupaciones de seguridad que se encuentran en las aplicaciones de niebla enumeradas a continuación: avance web, acceso de radio virtualizado, medidores inteligentes, sistemas portátiles 5G, sistemas vehiculares y seguridad vial, marcos de servicios medicinales, trazabilidad de sustento, manejo de videos de observación, información del discurso, gestión de activos y recursos, interfaz cerebro-PC ampliada, respuesta a catástrofes, disminución de energía y entornos hostiles. Debido a que no todos los nodos de niebla están repletos de recursos, las aplicaciones pesadas que necesitan nodos con recursos limitados no son exactamente simples, en contraste con las centrales de información tradicionales. Dichas aplicaciones populares se centran en vehículos y atención médica. La codificación de información crítica puede mejorar la seguridad de las aplicaciones al tiempo que evoca API. Al mismo tiempo, si se conjura y transporta un número excesivo de API, pueden devorar un número excesivo de activos, lo que afecta negativamente el acceso típico a ellos e incluso hace que el sistema de aplicaciones quede inmóvil.

*Innovación de intercambio seguro:* esto ocurre cuando los datos se comparten entre numerosos sitios web, como la coordinación armoniosa entre los nodos de niebla y los servicios. Para compartir servicios en la niebla, las redes sociales pueden ser utilizadas de manera innovadora. En la niebla social, para respaldar los servicios de seguridad correctamente junto con un mecanismo que facilita la detección de multitudes, se ha avanzado un modelo innovador de prestación de servicios de seguridad [1].

## CAPITULO 6. MODELADO Y SIMULACIÓN FOG COMPUTING

Debido a la complejidad y costo de inversión para la aplicación de la computación en la niebla, es importante analizar los diferentes aspectos y niveles de servicio con los que estará trabajando, incluyendo la distribución de recursos, balanceo de carga, migración y consolidación. Por todo lo mencionado anteriormente se han desarrollado diferentes simuladores de ambientes fog generando ahorros antes de su funcionamiento, algunos ejemplos de simuladores son: FogNetSim++ y iFogSim, FogNetSim++: Este simulador es una herramienta diseñada para mostrar a los usuarios las diferentes configuraciones de una gran red de niebla Está diseñado en la parte superior de OMNeT++ [37], que es una herramienta de código abierto que proporciona una amplia biblioteca para simular las características de la red mediante simulación de eventos discretos.

FogNetSim++ permite a los investigadores incorporar modelos de movilidad personalizados y programación de nodos de niebla algoritmos, así como la gestión de los mecanismos de entrega [7].

### 6.1. IFOGSIM

Es una herramienta de simulación de ambientes fog que permite a los usuarios simular la infraestructura de la computación en la niebla, y ejecutar aplicaciones simuladas para medir el rendimiento en términos de latencia, consumo de energía y uso de la red [38]. Es una aplicación basada en CloudSim [39], [7].



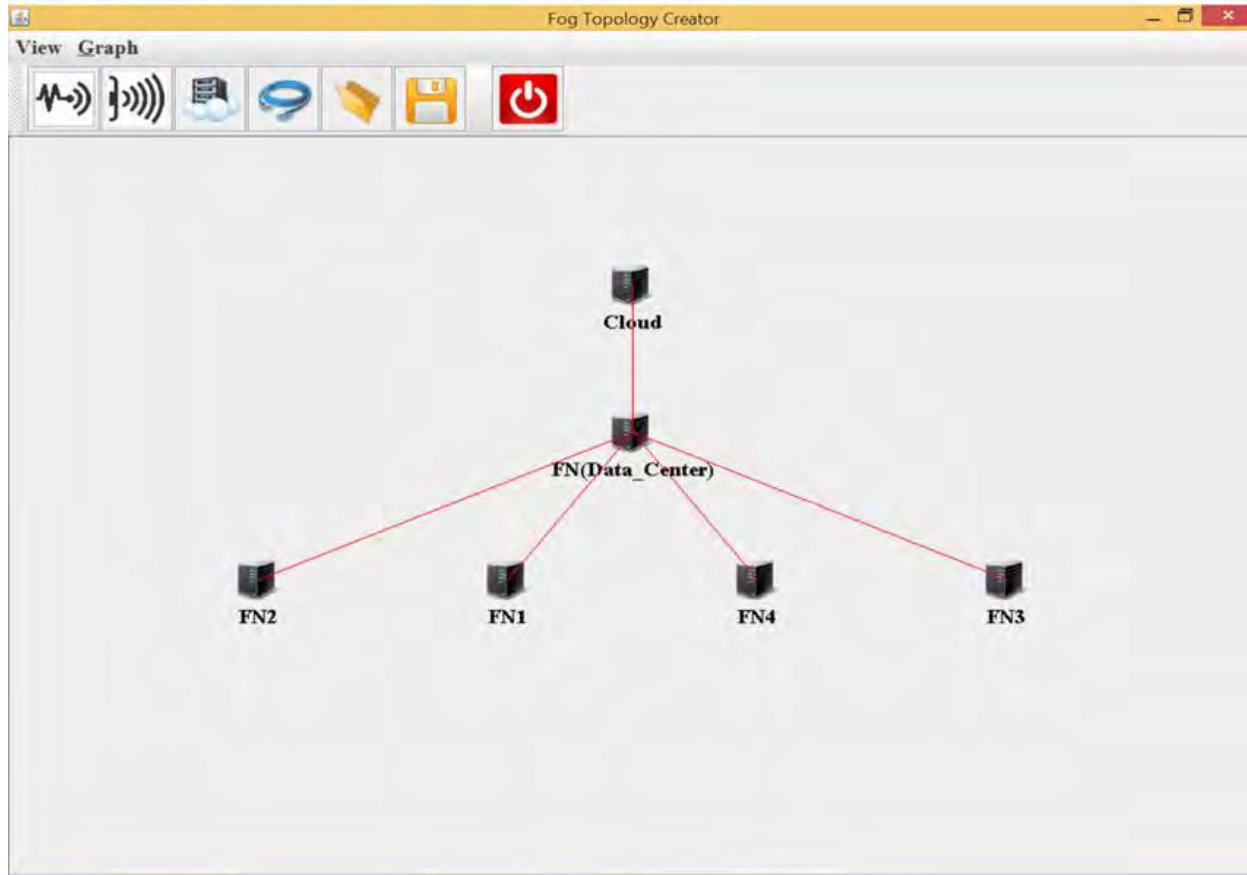


Ilustración 17 IFogSim fuente google

### 6.3. COMPUTACIÓN DE NIEBLA Y BORDE: DESAFÍOS DE MODELADO Y SIMULACIÓN

La creciente ubicuidad de las tecnologías móviles y los sensores conectados de bajo costo ha resultado en una avalancha de puntos finales computacionales y de redes en varios órdenes de magnitud en comparación a décadas anteriores. Las infraestructuras informáticas convencionales, incluida la informática en la nube, aprovechan los centros de datos geográficos centralizados utilizando hardware mercantilizado relativamente homogéneo. Dichas infraestructuras no fueron diseñadas para atender el procesamiento, almacenamiento y datos generados por miles de millones de puntos finales distribuidos, que operan en entornos a menudo dinámicos con conectividad de red intermitente. Como era de esperar, los proveedores de servicios se han enfrentado a desafíos sin precedentes para planificar y gestionar mayores demandas

y cumplir con los niveles mínimos de servicio. La computación en niebla ha surgido para complementar la computación en la nube. La computación de niebla se encuentra entre dispositivos finales inteligentes en el borde de las redes y los centros de datos o nube tradicionales. Desempeña un papel importante en la reducción de la congestión de la red y facilita el conocimiento de la ubicación, el soporte de movilidad, las interacciones en tiempo real, la escalabilidad y la interoperabilidad. En contraste, la computación de borde, en su sentido más puro, se define por la exclusión de la nube y la niebla, y se limita a un pequeño número de capas de red periférica. Tanto la computación de niebla como la de borde presentan desafíos importantes para los proveedores de servicios e investigadores, incluido el diseño y la implementación de la arquitectura de aplicaciones, la infraestructura y la administración de redes, la movilidad, la administración de recursos y la escalabilidad [4] [3].

### 6.3.1. MODELADO DE NIVEL DE APLICACIÓN

Existe una gama infinita de aplicaciones potenciales para la computación de niebla y de borde, que van desde el monitoreo de sensores basados en IoT simple hasta los complejos sistemas de procesamiento de datos inherentes a la Industria 4.0, salud electrónica, ciudades inteligentes, etc. En consecuencia, las aplicaciones subyacentes varían en función de sus necesidades sobre el grado de:

1. Conciencia de ubicación contextual y baja latencia.
2. Distribución geográfica.
3. Escala y coordinación de redes de punto final.
4. Heterogeneidad, interoperabilidad y funcionalidad de puntos finales.
5. En tiempo real vs procesamiento por lotes.
6. Movilidad de los puntos finales.
7. Interacción entre el borde, la niebla y las capas de nubes.

El aprovisionamiento para dicha heterogeneidad requiere una planificación significativa por adelantado y una optimización continua en todo el continuo C2T, incluido

el diseño de la aplicación. La mayoría de los servicios actuales de niebla y borde que admiten aplicaciones se pueden dividir en tres categorías principales: redes de distribución de contenido (CDN), IoT y funciones de red virtual (VNF). Si bien los tres usan la misma infraestructura, los aspectos funcionales de cada tipo de servicio son fundamentalmente diferentes. Los servicios de CDN se centran en la replicación y distribución de contenido estático en múltiples ubicaciones. Los servicios de IoT se utilizan para descargar el procesamiento y el almacenamiento de datos de los sensores a las ubicaciones de borde que empujan selectivamente algunos de los datos de la pila de red a la nube. Los VNF son cadenas de funciones de red que manejan el tráfico de protocolo de red móvil (por ejemplo, pila LTE) o proporcionan funciones de filtrado y enrutamiento de tráfico de red, como servicios empresariales, firewall y VPN. La ley sugiere que “siempre se debe desarrollar un modelo de simulación para un conjunto particular de objetivos. De hecho, un modelo que sea válido para un objetivo puede no serlo para otro”. Modelar todas las aplicaciones implementadas dentro de una red de niebla / borde puede ser beneficioso para los proveedores de infraestructura, pero construir una solución de simulación que pueda manejar eficientemente un conjunto de aplicaciones tan amplias, es un desafío y necesita una cuidadosa consideración [7] [3].

#### 6.4. INFRAESTRUCTURA Y MODELADO A NIVEL DE RED

Debido a la dependencia de la comunicación en la nube y a los grandes volúmenes de datos generados por las aplicaciones de niebla y edge, la conectividad y la capacidad de la red pueden ser una limitación significativa, especialmente en el caso de aplicaciones sensibles al retraso en tiempo real. Este es particularmente el caso en el borde móvil. La gestión de la movilidad es crítica en la informática de borde móvil (MEC), especialmente en entornos altamente dinámicos. Para gestionar la demanda en escenarios MEC, se implementan cantidades masivas de celdas pequeñas. En este escenario, el rango de usuario puede ser muy limitado y, por lo tanto, las transferencias son más frecuentes, lo que resulta en una carga pesada en la red [7].

Los dispositivos de niebla y borde utilizan una amplia variedad de tecnologías de comunicación, que van desde protocolos tradicionales de bajo costo, como IEEE 802.11

hasta protocolos de eficiencia energética, como IEEE 802.15.4 (ZigBee / 6LoWPAN) y Bluetooth Low Energy (LE). Cada una de estas tecnologías tiene un impacto en el rendimiento del punto final directamente, ya sea el procesamiento de datos, el tiempo de servicio, el retraso de la transferencia de datos, etc. Llegar a la tecnología óptima de acceso a la red, generalmente implica una compensación entre el rendimiento y el costo y, a menudo, está fuera del control del proveedor de servicios [7].

Los modelos de sistemas de niebla y borde pueden extenderse a miles de ubicaciones de sitios distribuidos creando una red de recursos que abarca varios países. Cada sitio puede estar compuesto por equipos informáticos y de red que alojan múltiples aplicaciones a las que pueden acceder los usuarios del servicio perimetral. Crear tal modelo a mano, incluso a un nivel de abstracción más alto, ya no es práctico desde una perspectiva de tiempo y esfuerzo. Para resolver el problema, se requiere un enfoque automatizado para la construcción de modelos. La integración con un sistema de monitoreo de recolección de datos puede abordar parcialmente el desafío al tomar un momento de estado de una infraestructura existente. Sin embargo, para construir modelos significativos de comportamiento del sistema, los datos de monitoreo deben someterse a un procesamiento adicional para extraer las tendencias de comportamiento de la carga de trabajo y las demandas de recursos de la aplicación. Tal proceso pone en juego la gestión de grandes datos y los desafíos de procesamiento que requieren un mayor desarrollo dentro del alcance del dominio de simulación [7].

## 6.5. MOVILIDAD

Estudios recientes se centran en la aparición de redes 5G y la interacción entre estas redes y la computación de niebla y borde. Las redes 5G ofrecen mejoras de red a través de la optimización del uso de recursos móviles, el preprocesamiento de datos de gran tamaño y los servicios conscientes del contexto (utilizando la carga celular, la ubicación del usuario y el ancho de banda asignado como información). A pesar de estas mejoras, dado que cada aplicación de niebla y borde puede tener diferentes requisitos de latencia y puede generar diferentes tipos de datos y tráfico de red, puede ser necesario un mecanismo para diferenciar los flujos sensibles al retraso, como el corte de la red [7].

El modelado de los aspectos de movilidad del usuario requiere la implementación de una lógica de conocimiento geográfico, por ejemplo, el cálculo del punto de acceso móvil más cercano basado en las coordenadas del usuario en cada paso de tiempo de simulación. Además, la disponibilidad y el acceso a datos del mundo real sobre la movilidad del usuario final es problemático tanto legal como técnicamente. Los cálculos adicionales aumentan aún más la complejidad y la demanda de recursos computacionales de una plataforma de simulación dada. Los generadores de modelos inteligentes son una solución para crear modelos de carga de trabajo de infraestructura de niebla y borde basados en datos sociodemográficos y geográficos de terceros que pueden usarse para fines de simulación [7].

## 6.6. ADMINISTRACION DE RECURSOS

La mayoría de los escenarios 4IR, Industry 4.0 e IoT asumen la generación, captura y análisis de datos en volúmenes, variedades y velocidades de órdenes de magnitud mayores que antes. Estos datos pueden incluir información útil si se puede identificar dicha información. Por ejemplo, un sistema básico de vehículo conectado puede generar decenas de megabytes de datos por segundo. La provisión de infraestructura de manera eficiente y efectiva requiere varias decisiones clave, entre ellas, cómo se recopilarán los datos, dónde y cómo se procesarán los datos (borde, niebla o nube), y con qué frecuencia los datos deben enviarse a la nube a largo plazo de almacenamiento o análisis posterior. Existen dos presiones competitivas que informan estas decisiones: el uso de la infraestructura y la calidad de servicio del usuario final.

Los sistemas de procesamiento de eventos complejos (CEP) se citan cada vez más para procesar y analizar grandes volúmenes de datos y detectar eventos de interés cuando ocurren. Sin embargo, la tarea de CEP puede llevar mucho tiempo y, por lo general, los dispositivos de niebla o borde presentan limitaciones de capacidad de almacenamiento y computación, en comparación con la capacidad de la nube. Como tal, el almacenamiento en caché se usa ampliamente para llevar la funcionalidad de almacenamiento a los bordes de la red con una latencia más baja, un consumo de ancho de banda menos excesivo y tiempos de transmisión reducidos. Este es particularmente el caso de los casos de uso de distribución de contenido, como el video IP, que se prevé

que represente una parte significativa de todo el tráfico IP en los próximos años. Wang et al. resumen los principales desafíos en el almacenamiento en caché de contenido en redes perimetrales como la colocación en caché, la popularidad del contenido, las políticas y algoritmos de almacenamiento en caché y el conocimiento de la movilidad [7].

Comprender la generación de carga de datos y su propagación a través de un sistema dado es un enfoque valioso para decidir sobre la colocación (óptima) de recursos. La predicción de carga de datos se ha presentado como una solución para la corrección proactiva del sistema. En este caso, los datos históricos (grandes) almacenados en la nube y los datos en vivo recopilados en los dispositivos de niebla y borde se usan para alimentar modelos y predecir métricas importantes, como el uso de recursos y la distribución de popularidad de contenido. Las técnicas de aprendizaje automático también se han utilizado ampliamente para resolver este problema. Por ejemplo, Zeydan et al. utilizan el aprendizaje automático para predecir el comportamiento del usuario espaciotemporal para decisiones de almacenamiento en caché proactivo con el objetivo de satisfacer la demanda del usuario al ofrecer baja latencia y mayor QoE.

Noor et al. identificaron la eficiencia energética como uno de los desafíos importantes para la gestión de recursos móviles en la nube. Por ejemplo, si bien la descarga del procesamiento de datos a la nube puede reducir el consumo de batería del dispositivo, aumenta el uso del ancho de banda de la red y el consumo de energía, un contribuyente significativo al aumento del consumo de energía. Como era de esperar, la eficiencia energética es un foco principal de la investigación de computación en la nube, la niebla y el borde, incluida la optimización de las asignaciones de recursos bajo restricciones de energía, rendimiento y QoS. La computación en niebla puede introducir flexibilidad de administración al proporcionar más opciones para el procesamiento de datos dentro de la jerarquía de red distribuida. Desde la perspectiva de la nube, decidir si almacenar en caché o procesar la descarga de datos es una forma de aliviar la congestión de la red y reducir los costos de transferencia de datos; desde la perspectiva de un dispositivo periférico, la descarga de algunas tareas informáticas podría mejorar el rendimiento del servicio y ser más eficiente en cuanto a la energía, ya que algunos dispositivos periféricos están muy limitados. Como tal, el perfil de rendimiento del dispositivo de borde debe tenerse en cuenta, especialmente para aplicaciones sensibles

en tiempo real, como comunicaciones de vehículo a vehículo, comunicaciones de vehículo a carretera y aplicaciones de comercio financiero en tiempo real que pueden requerir latencias por debajo de decenas de milisegundos. Por lo general, se requieren experimentos intensivos de rendimiento de referencia para decidir la mejor configuración de niebla a borde teniendo en cuenta una variedad de factores que incluyen la capacidad computacional y de almacenamiento, la duración de la batería, la movilidad, la interfaz de comunicación, etc. La importancia de la disponibilidad del sistema para tales dispositivos puede ser una consideración importante particularmente en casos de uso donde la pérdida de datos o la interrupción del servicio pueden dar lugar a resultados adversos para los usuarios finales, por ejemplo, en los sistemas de monitoreo de la atención médica.

El tiempo de ejecución, la capacidad de programación y la interoperabilidad de los dispositivos de borde a menudo difieren debido a su heterogeneidad que resulta en problemas de descarga de datos. El Instituto Europeo de Normas de Telecomunicaciones (ETSI), el Consorcio OpenFog y otros están tratando de abordar la estandarización para la computación de borde de acceso múltiple, sin embargo, tales iniciativas se encuentran en una etapa temprana de desarrollo y enfrentan desafíos cuesta arriba contra la avalancha de nuevos puntos finales conectados que se están introduciendo [7].

El enfoque de simulación ha demostrado ser un esfuerzo valioso para probar la asignación y gestión de recursos en la nube. En su estudio, Stier et al. presenta una integración directa entre el marco de simulación y optimización que se implementó para probar los algoritmos de gestión de recursos disponibles que pueden usarse directamente dentro de un sistema real. Además, la simulación también se puede utilizar como parte de algoritmos de gestión de recursos para reducir el espacio de búsqueda para las soluciones óptimas en una técnica de optimización conocida como recocido simulado (SA). SA es un algoritmo de optimización que utiliza un enfoque de búsqueda local para moverse alrededor de los valores vecinos en un espacio de búsqueda definido hasta encontrar la solución óptima. Aunque la técnica de recocido simulada sale del alcance tradicional de la simulación de eventos discretos (DES), el enfoque de recocido general puede ser útil para probar diferentes variaciones de parámetros dentro de la

computación perimetral, como las implementaciones de la red de entrega de contenido virtual (vCDN) o explorar las opciones de aprovisionamiento de infraestructura. Pasando al dominio de niebla y borde, la necesidad de simular enfoques de gestión de recursos sigue siendo una de las principales características de análisis de simulación [7].

## 6.7. ESCALABILIDAD

La elección de una herramienta de simulación depende significativamente del tipo de aplicaciones. Este hecho también dicta la granularidad de la simulación. Por ejemplo, los fenómenos macroscópicos, como las estrategias de enrutamiento, se pueden estudiar a nivel de paquete, utilizando el enfoque DES. A pesar de esto, una simulación muy precisa podría obstaculizar sustancialmente el rendimiento y conducir a resultados similares a otros métodos de rendimiento más rápido. Otro punto clave al considerar un marco de simulación es la generalidad de la gama de fenómenos y aplicaciones que pueden simularse. Los marcos de simulación más generales generalmente no se centran en características específicas, sino en una gran cantidad de parámetros que pueden no ser requeridos por el usuario y pueden ser muy complejos de configurar y operar. Estos marcos tienden a cubrir una amplia variedad de aplicaciones y fenómenos. Por otro lado, las soluciones de simulación dedicadas suelen ser más fáciles de usar, adaptadas y optimizadas para aplicaciones específicas y su complejidad. Sin embargo, las soluciones dedicadas no son fácilmente adaptables a otras aplicaciones, sin un esfuerzo de desarrollo significativo. En el análisis de los marcos de simulación existentes para la computación de niebla y borde, muchos son extensiones de CloudSim y sufren sus limitaciones en términos de escala y enfoque. Otros se centran en escenarios de casos de uso específicos. Estas presentan limitaciones a corto plazo para los investigadores de computación en la nube y en la niebla, pero también oportunidades para la investigación de simulación [7].

Experimentar con sistemas a gran escala requiere que los recursos informáticos estén disponibles para que un marco de simulación lo use. DES es el enfoque más popular utilizado en la computación en la nube, como se refleja en el análisis anterior. Sin embargo, la naturaleza secuencial de la cola de eventos es notoriamente difícil de paralelizar ya que cada evento puede cambiar el estado del sistema. Por lo tanto, si un



evento se procesa fuera de servicio, el cálculo puede ser incorrecto. Dicho esto, donde uno puede hacer divisiones claras dentro del modelo, los eventos de simulación se pueden procesar en grupos independientes que aumentan el grado de paralelismo. Por ejemplo, Varga y Sekercioglu discuten un enfoque paralelo de simulación de eventos discretos (PDES) que es capaz de distribuir la simulación en múltiples procesadores y máquinas, evitando también cuellos de botella en la memoria al dividir el modelo entre máquinas. Otro ejemplo es Cloud2Sim, una extensión del popular framework CloudSim que utiliza Hazelcast e Infinispan en almacenes de datos distribuidos en memoria. La ejecución paralela de DES no se adopta ampliamente en las herramientas de simulación de bordes recientemente lanzadas que limitan su rango de aplicación [7].

El enfoque de simulación de tiempo discreto (DTS) se puede utilizar para tratar de combatir las dificultades de paralelización asociadas con DES. DTS utiliza el concepto de paso de tiempo para actualizar el estado de los componentes del sistema, evitando la necesidad de cálculo previo y almacenamiento de eventos futuros. Este enfoque presenta una reducción significativa de los requisitos de memoria del simulador y mejora el rendimiento al tiempo que permite el procesamiento paralelo y, junto con los requisitos de memoria reducidos, proporciona un mecanismo para la simulación de redes muy grandes. El estado de todos los componentes involucrados en una simulación, por ejemplo, sitios, nodos, máquinas virtuales, etc., se puede actualizar en paralelo, ya que no hay dependencias entre los componentes, lo que mejora la escalabilidad. El cambio de estado de los componentes constituyentes solo se ve afectado por las solicitudes de entrada. Este enfoque simplifica sustancialmente el diseño e incorporación de modelos avanzados de consumo de energía y estrategias para la formación de rutas en redes. Además, la granularidad de la simulación se controla mediante la elección del paso de tiempo: la elección de un paso de tiempo más pequeño da como resultado un número muy grande de pasos de tiempo, lo que potencialmente aumenta la precisión de la simulación y al mismo tiempo dificulta el rendimiento. Un paso de tiempo grande típicamente resulta en un submuestreo del fenómeno estudiado descuidando los fenómenos transitorios que podrían afectar sustancialmente el resultado de la simulación. La simulación DTS se ha utilizado en el contexto de la simulación a gran escala de entornos de nube tradicionales y basados en self \* en entornos de

supercomputación. Los enfoques DES y DTS tienen puntos fuertes y débiles en comparación entre sí. Generalmente se considera que DES es una herramienta adecuada cuando se aplica a un problema que requiere un enfoque de modelado más granular que es más difícil de escalar, mientras que DTS generalmente permite el modelado de sistemas a gran escala con un esfuerzo relativamente menor, pero con la posibilidad de un mayor grado de inexactitud. Ambos paradigmas pueden aplicarse al dominio de niebla y borde dependiendo de los objetivos de experimentación [7].

En términos de precisión, existen desafíos en relación con la validación de sistemas a gran escala, ya que la simulación representa un modelo abstracto de un entorno real, por lo tanto, es imperativo que el nivel de abstracción no impida la precisión del resultado de la simulación. El proceso de validación de simulación asegura que los experimentos de simulación produzcan estimaciones confiables del comportamiento del sistema. Los enfoques existentes sugieren validar los modelos de simulación con expertos en el dominio para garantizar los atributos de validez aparente del modelo y las restricciones de comportamiento. Además, los resultados de la simulación deben validarse comparando los resultados simulados con los datos del sistema real monitoreados, por ejemplo, comparando visualmente los resultados simulados y monitoreados graficados lado a lado o comparando estadísticamente la distribución de datos, por ejemplo, utilizando un enfoque de prueba t. Validar los modelos y resultados de simulación no es un desafío nuevo, sin embargo, aplicar técnicas de validación a simulaciones de computación de niebla y borde puede ser un desafío. En primer lugar, es difícil inspeccionar el entorno objetivo debido al tamaño y la complejidad. En segundo lugar, la falta de acceso a datos reales impacta la validación en comparación. Las metodologías de validación automáticas o semiautomáticas capaces de procesar grandes volúmenes de datos pueden resolver o aliviar los desafíos de validación comprobando la coherencia y las anomalías de los resultados de los datos del modelo [7].

## 6.8. ESTUDIO ACERCA HERRAMIENTAS DE MODELADO FOG AND EDGE

Según Dastjerdi y Buyya, para permitir el análisis en tiempo real en la computación de niebla y de borde a nivel de software, debemos preocuparnos por las diferentes

técnicas de gestión y programación de recursos, incluida la distribución de recursos, el equilibrio de carga, la migración y la consolidación. En la capa física, los sistemas de niebla y borde tienen muchos requisitos adicionales que deben abordarse, como la conectividad y la capacidad de la red. Esta escala y complejidad de los sistemas C2T hace que el uso de prototipos realistas sea inviable. Del mismo modo, los proveedores de servicios comerciales generalmente no brindan el acceso o el control de infraestructura necesarios a terceros para probar las técnicas antes mencionadas y la construcción de un banco de pruebas con un alto grado de verosimilitud es complejo, costoso, requiere mucho tiempo y recursos. Para superar estos problemas, los marcos de simulación proporcionan un medio de costo relativamente bajo para comprender y evaluar los sistemas de niebla y borde y eliminar políticas y estrategias ineficaces.

La simulación se ha utilizado ampliamente para simular las infraestructuras de red tradicionales, como las redes inalámbricas de sensores (WSN) convencionales. Algunos ejemplos de estos simuladores son NS-2, TOSSIM, EmStar, OMNeT ++, J-Sim, ATEMU y Avrora. Estos simuladores se utilizan universalmente para desarrollar y probar protocolos de red, especialmente en la etapa de diseño inicial. No fueron diseñados teniendo en cuenta los entornos informáticos de niebla y edge; como tal, están fuera del alcance de este documento. Redirigimos al lector a una encuesta detallada para obtener más información sobre estos simuladores. Si bien existe una amplia gama de simuladores para la computación en la nube, hay relativamente pocos que se puedan usar para simular escenarios de computación de niebla y borde. A continuación, describimos brevemente una selección de simuladores prominentes utilizados para modelar niebla y bordes y los comparamos en términos cualitativos.

FogNetSim ++ es una herramienta de simulador de niebla que proporciona a los usuarios opciones de configuración detalladas para simular una gran red de niebla. Está diseñado en la parte superior de OMNeT ++, que es una herramienta de código abierto que proporciona una amplia biblioteca para simular características de red utilizando simulación de eventos discretos.

FogNetSim ++ permite a los investigadores incorporar modelos de movilidad personalizados y algoritmos de programación de nodos de niebla, así como gestionar mecanismos de transferencia. Se evalúa un sistema de gestión de tráfico para demostrar

la escalabilidad y efectividad del simulador FogNetSim ++ en términos de uso de CPU y memoria. Los autores proporcionan un punto de referencia de los parámetros de red, como el retraso de ejecución, la tasa de error de paquetes, los trasposos y la latencia. Sin embargo, FogNetSim ++ aún no admite la migración de VM entre nodos de niebla.

iFogSim es un juego de herramientas de simulación de computación de niebla que permite a los usuarios simular infraestructuras de computación de niebla y ejecutar aplicaciones simuladas para medir el rendimiento en términos de latencia, consumo de energía y uso de la red. iFogSim se basa e implementa en CloudSim. iFogSim permite el modelado y la simulación de entornos informáticos de niebla para evaluar la gestión de recursos y las políticas de programación. Mide las métricas de rendimiento y simula dispositivos periféricos, centros de datos en la nube, sensores, enlaces de red, flujos de datos y aplicaciones de procesamiento de flujo. Además, iFogSim integra servicios simulados para el monitoreo de energía y la administración de recursos en dos niveles separados, es decir, la ubicación de la aplicación y la programación de la aplicación. Se empaquetan dos estrategias de colocación de módulos de aplicación para admitir múltiples escenarios de implementación, a saber, (a) colocación solo en la nube, donde todos los módulos de aplicaciones se ejecutan en centros de datos y (b) colocación de borde, donde los módulos de aplicación se ejecutan en nodos de niebla cerca del borde dispositivos. Además, hay extensiones disponibles para respaldar el diseño de estrategias de colocación de datos de acuerdo con objetivos específicos, como la minimización de la latencia del servicio, la congestión de la red y el consumo de energía. También vale la pena señalar que, dado que el paradigma de la computación en la niebla tiene muchas similitudes con la computación en la nube, CloudSim también se puede usar como una aplicación independiente para implementar muchas características de la computación en la niebla. iFogSim no está exento de limitaciones. Si bien permite la definición de la ubicación de los dispositivos que reciben servicio de los servidores de niebla, esta información es estática y ningún modelo de movilidad la actualiza. Además, si bien se basa en Cloudsim ofrece ventajas, iFogSim está limitado a DES y su escalabilidad es limitada. Tanto EdgeCloudSim como IOTsim, como iFogSim, también se basan en CloudSim. EdgeCloudSim está específicamente diseñado para evaluar las necesidades computacionales y de redes de la computación perimetral. A diferencia de

iFogSim, EdgeCloudSim admite movilidad. De hecho, proporciona el modelo de movilidad, el modelo de enlace de red y el modelo de servidor perimetral para evaluar las diversas facetas de la informática perimetral. Además de sus capacidades de simulación, EdgeCloudSim es relativamente fácil de usar y proporciona un mecanismo para obtener la configuración de dispositivos y aplicaciones de los archivos XML en lugar de definirlos mediante programación. IOTSim fue diseñado para simular entornos informáticos de borde donde la aplicación IoT envía grandes volúmenes de datos a un gran sistema de procesamiento de datos. Como tal, agrega un almacenamiento y la capa de procesamiento de big data en CloudSim. En la capa de almacenamiento, la red y los retrasos de almacenamiento se simulan para aplicaciones IoT. La capa de procesamiento de datos grandes simula MapReduce para admitir el paradigma de procesamiento de datos orientado a lotes. Tanto EdgeCloudSim como IOTsim heredan la misma escalabilidad y limitaciones de DES que iFogSim.

Brogi et al. recientemente presentaron un prototipo de simulador, FogTorchII, que amplía su trabajo anterior, (FogTorch). Diseñado principalmente para admitir el despliegue de aplicaciones en la niebla, FogTorchII es un simulador de código abierto desarrollado en Java. Es capaz de evaluar las implementaciones de infraestructura de computación de niebla, modela capacidades de software (sistema operativo, lenguajes de programación, marcos, etc.), capacidades de hardware (núcleos de CPU, RAM y almacenamiento) y atributos de QoS incluyendo latencia y ancho de banda. FogTorchII utiliza simulaciones de Monte Carlo para implementar variaciones en los enlaces de comunicaciones utilizados como entradas. El resultado final consiste en los resultados agregados en términos de garantía de QoS y consumo de recursos de niebla a través de un indicador del porcentaje de RAM y almacenamiento consumidos. Una limitación importante y reconocida de FogTorchII es la escalabilidad, un problema que Brogi et al. espero abordar explotando la heurística para reducir el espacio de búsqueda. Las simulaciones hacen varias simplificaciones que pueden no ser siempre ciertas, especialmente con una infraestructura tan dinámica como la computación de niebla y edge. Como tal, se desarrollaron varios marcos de emulación para abordar esta limitación. EmuFog es un marco de emulación extensible diseñado para escenarios de computación de niebla. EmuFog permite el diseño de infraestructuras de cómputo de

niebla ab initio y la emulación de aplicaciones y cargas de trabajo reales a gran escala que permite a los desarrolladores implementar y evaluar su comportamiento, así como la carga de trabajo inducida en la topología de la red. El proceso de implementación en EmuFog consta de cuatro etapas:

1. Una topología de red se genera o carga desde un archivo, lo que admite conjuntos de datos de topología del mundo real.
2. La topología de la red se convierte en un gráfico no dirigido, donde los nodos representan dispositivos de red (por ejemplo, enrutadores) y los enlaces corresponden a las conexiones entre ellos.
3. Se determinan los dispositivos de borde y los nodos de niebla se colocan de acuerdo con una política de colocación. Los usuarios pueden definir las capacidades computacionales de los nodos de niebla, así como la cantidad de clientes que se espera que atienda cada nodo.
4. Los nodos de niebla se emulan desde el entorno emulado de red, mientras que las aplicaciones en cualquier nodo de niebla individual se ejecutan en contenedores Docker.

A pesar de la utilidad de EmuFog, el marco no admite movilidad tanto para clientes como para nodos de niebla. Además, EmuFog no admite infraestructuras jerárquicas de niebla. Fogbed es otro emulador que extiende el marco Mininet del emulador de red para permitir el uso de contenedores Docker como nodos virtuales. Proporciona capacidades para construir bancos de pruebas en la nube y la niebla. La API Fogbed permite agregar, conectar y eliminar contenedores dinámicamente de la topología de la red. Estas características permiten la emulación de infraestructuras de nube y niebla del mundo real en las que se pueden iniciar y finalizar instancias de cómputo en cualquier momento. Además, es posible cambiar las limitaciones de recursos en tiempo de ejecución para un contenedor, como el tiempo de CPU y la memoria disponible. Sin embargo, Fogbed aún

no admite aspectos clave de la computación de niebla, incluida la seguridad, la tolerancia a fallas, la escalabilidad y la administración de confiabilidad.

Las herramientas del simulador anteriores contra seis atributos cualitativos clave:

1. Paradigma informático (sistema de destino).
2. Modelado a nivel de infraestructura.
3. Modelado a nivel de aplicación.
4. Modelado de gestión de recursos.
5. Movilidad.
6. Escalabilidad.

En resumen, a pesar de un mayor interés en la computación de niebla y borde, la investigación sobre marcos de simulación adecuados para respaldar los requisitos de este dominio está rezagada (ver Tabla 5). La mayoría de las herramientas de simulación existentes, aunque sea un número pequeño, ponen un mayor énfasis en la computación de niebla. Tienen limitaciones significativas en escalabilidad y soporte de movilidad. Todos los simuladores existentes utilizan DES en su núcleo y la dependencia de CloudSim para tres de los simuladores les impone una limitación adicional, particularmente en términos de escalabilidad. Por lo tanto, existe una necesidad urgente de herramientas de simulación con una mayor cobertura de las características de la computación de niebla y borde. Ficco et al. argumentan que los entornos puramente simulados y los bancos de pruebas reales no son suficientemente representativos de los escenarios del mundo real y / o son inaceptablemente caros. Como tal, sugieren que un enfoque de prueba pseudodinámica híbrida puede aumentar la verosimilitud simulando una parte del escenario experimental, al tiempo que emula los nodos de borde y niebla bajo prueba o los ejecuta en un entorno real [7].

Tabla 5.- Herramientas de simulador niebla y borde: estudio comparativo.

Atributos	FogNetSim ++	iFogSim	FogTorchII	EdgeCloudSim m	IOTSim	EmuFog	Fogbed
Paradigma de computación (sistema de destino)	Computación de niebla (general)	Computación de niebla (general)	Computación de niebla (general)	Edge computing (IoT)	Edge computing (IoT)	Computación de niebla (general)	Computación de niebla (general)
Infraestructura y modelado a nivel de red	Centros de datos distribuidos Sensores Nodos de niebla Corredor Enlaces de red Retraso Trasposos Banda ancha	Centros de datos en la nube Sensores Actuadores Dispositivos de niebla Enlaces de red Retraso Uso de la red Consumo de energía	Latencia Banda ancha	Centros de datos en la nube Enlaces de red Servidores perimetrales WLAN y LAN delay Banda ancha	Centro de datos en la nube Latencia Banda ancha	Enlaces de red Nodos de niebla Enrutadores	Nodos virtuales Interruptores API de instancia Enlaces de red
Modelado a nivel de aplicación	Fog Network	Flujo de datos Procesamiento de flujo	Aplicaciones Fog	Mobile edge	IoT	Fog	Fog Network



Modelado de gestión de recursos	Consumo de recursos (RAM y CPU)	Consumo de recursos El consumo de energía Políticas de asignación	Consumo de recursos (RAM y almacenamiento)	Consumo de recursos (RAM y CPU) Fallo debido a la movilidad.	Consumo de recursos (RAM, CPU y almacenamiento)	Carga de trabajo	Consumo de recursos (RAM y CPU) Banda ancha Carga de trabajo
Movilidad	Si	No	No	No	No	No	No
Escalabilidad	Si	No	No	No	Si (reducción de mapa)	No	No

## CAPITULO 7. DESAFÍOS Y DIRECCIONES FUTURAS DE INVESTIGACIÓN.

### 7.1. SISTEMA DE NIEBLA SLA.

Los acuerdos de nivel de servicio (SLA) no están definidos actualmente para los sistemas de niebla. Los SLA actuales que se usan para sistemas de niebla se definen para servicios en la nube (por ejemplo, garantía de disponibilidad del 99,99% para servicios en la nube) o infraestructura de red. Además, un sistema de niebla puede tener múltiples proveedores / operadores y abarcar múltiples dominios operativos. Una posible dirección de investigación es definir un SLA nuevo y compatible para los sistemas de niebla (por ejemplo, garantizar la latencia y el ancho de banda). Además, el diseño de las técnicas de administración de SLA y el marco para la computación de niebla que admite múltiples proveedores o proveedores es otra dirección potencial [2] [4] [3].

### 7.2. DISEÑO DE SISTEMA DE NIEBLA MULTIOBJETIVO.

La mayoría de los esquemas existentes que se proponen para los sistemas de niebla, como la descarga, el equilibrio de carga o el suministro de servicios, solo consideran pocos objetivos (por ejemplo, QoS, costo) y asumen que otros objetivos no afectan el problema. Una nueva dirección de investigación será diseñar esquemas que consideren muchos objetivos (por ejemplo, QoS, ancho de banda, energía, costo) simultáneamente. Por ejemplo, desarrollar un esquema de descarga de tareas eficiente que considere el ancho de banda, el tiempo de espera, la disponibilidad, la seguridad y la energía al mismo tiempo es una dirección prometedora [3].

### 7.3. DISEÑO DE SISTEMA DE NIEBLA CON RECONOCIMIENTO DE ANCHO DE BANDA

Pocos estudios consideran el ahorro de ancho de banda mediante el uso de la computación de niebla, a pesar de que una de las características prometedoras de la computación de niebla es reducir el uso de ancho de banda en el núcleo de Internet. Existe la necesidad de más investigación sobre el ahorro de ancho de banda mediante

el uso de la computación de niebla. Estos estudios podrían ser estudios de medición que capturan el uso real del ancho de banda en presencia de la computación de niebla [3].

#### 7.4. DISEÑO ESCALABLE DE ESQUEMAS DE NIEBLA

Muchos de los esquemas y algoritmos existentes para la niebla no se ajustan a la magnitud de las redes IoT, ya que los autores descuidan la escalabilidad en su diseño fundamental. Creemos que la escalabilidad es crítica en el diseño de sistemas de niebla; Los sistemas de niebla deben ser escalables para que puedan implementarse en redes IoT. Por ejemplo, un algoritmo escalable para la descarga de niebla es un esquema de descarga en línea que no necesita información de nodos de IoT individuales para la toma de decisiones. Alentamos a los investigadores en el área de cómputo de niebla a verificar la escalabilidad de sus algoritmos y esquemas propuestos (por ejemplo, mediante una implementación real) [3].

#### 7.5. COMPUTACIÓN DE NIEBLA MÓVIL

La mayor parte de la literatura existente supone que los nodos de niebla son fijos, o solo considera la movilidad de los dispositivos IoT. Se ha prestado menos atención a la computación de niebla móvil y cómo los nodos de niebla móviles pueden mejorar la QoS, el costo y el consumo de energía. Cuando los nodos de niebla son móviles, la disponibilidad de recursos de niebla, el descubrimiento de recursos, la descarga de tareas y el aprovisionamiento de recursos serán más desafiantes. La computación de niebla móvil, donde los nodos de niebla pueden moverse y formar nuevas redes, es una dirección de investigación interesante y desafiante. Además, diseñar un esquema para la gestión o federación de nodos de niebla móviles es otra dirección posible. Junto con la computación de niebla móvil, es necesario que existan nuevos métodos de aprovisionamiento para los servicios de niebla móviles, de modo que los servicios de niebla estén disponibles para los nodos y usuarios de IoT. Del mismo modo, se podría diseñar un esquema de descarga y programación de tareas cuando los nodos de niebla son móviles [3].

## 7.6. MONITOREO DE RECURSOS DE NIEBLA

Pocos estudios en la literatura proponen esquemas de monitoreo para los recursos de niebla. El monitoreo es útil cuando varios operadores usan un nodo de niebla, o cuando un nodo de niebla se encuentra en una ubicación donde muchos usuarios usan el nodo de niebla. Una posible dirección es desarrollar técnicas de monitoreo de recursos de niebla que admitan el acceso de múltiples operadores. El uso del software de monitoreo basado en SDN para el monitoreo de recursos de niebla y el anuncio de recursos de niebla también es un enfoque prometedor [3].

## 7.7. COMPUTACIÓN DE NIEBLA VERDE

Pocos estudios en la literatura revisada han abordado el criterio de energía en el diseño de su sistema. La mayoría de los estudios sobre energía se refieren a la descarga de cómputo consciente de la energía, la gestión de la movilidad consciente de la energía y la federación de dispositivos IoT para mejorar el consumo de energía de los sistemas de niebla. Sin embargo, mejorar el consumo general de energía de la niebla no ha sido bien estudiado. El consumo de energía de una red de niebla incluye tres porciones principales:

- 1) consumo de energía de dispositivos IoT que envían datos a la niebla.
- 2) consumo de energía de la red que interconecta dispositivos IoT y los nodos de niebla.
- 3) consumo de energía de los nodos de niebla.

Para reducir el consumo de energía de los dispositivos IoT, el uso de recolectores de energía y el almacenamiento de baterías para dispositivos y sensores IoT son posibles direcciones de investigación. Los recolectores de energía pueden mejorar el consumo de energía al tiempo que presentan nuevos desafíos para el sistema, como la incertidumbre y la imprevisibilidad. Para reducir el consumo de energía de la red que interconecta los dispositivos IoT y los nodos de niebla, una de las posibles direcciones

de investigación es identificar dónde colocar los nodos de niebla y qué tan cerca deberían estar de los usuarios finales. Los nodos de niebla móviles también son un caso de uso convincente para el consumo de energía. Para reducir el consumo de energía de los nodos de niebla, una posible dirección de investigación es reducir la distancia entre los servidores de niebla y las fuentes locales de energía renovable (como la solar, la eólica o la vibración). Este problema se puede abordar de diferentes maneras: el tráfico de los dispositivos IoT se puede redirigir al nodo de niebla más cercano que funciona con energía renovable. La otra forma es que las compañías de telecomunicaciones identifiquen la ubicación de los nodos de niebla que necesitan la gran cantidad de energía para atender el tráfico, y alentar a las personas a usar su energía renovable local para su micro-red local para encender sus nodos de niebla locales [3].

#### 7.8. SOPORTE SDN PARA NIEBLA

El software SDN no tiene soporte nativo para la computación en niebla. SDN es principalmente comercialmente viable dentro de grandes centros de datos o redes de campus [9]. Mejorar y estandarizar el software SDN (p. Ej., Interfaz de flujo abierto hacia el norte, sur, este-oeste) para casos de uso de niebla es una dirección que creemos que facilitará el desarrollo del software de cómputo de niebla. Además, con múltiples proveedores / operadores en sistemas de niebla, habrá una necesidad de nuevas arquitecturas SDN con múltiples dominios y jerarquías de controladores SDN [3].

#### 7.9. SOPORTE DE USUARIOS DE ALTA VELOCIDAD

Los protocolos de comunicación actuales que se proponen para entornos de niebla no admiten usuarios de alta velocidad, como usuarios de automóviles, usuarios de trenes y computación vehicular. Una dirección de investigación es desarrollar protocolos de autenticación y apretón de manos rápidos o sin estado para usuarios de alta velocidad y comunicación automotriz. Tenga en cuenta que ya se han realizado algunos esfuerzos iniciales en este campo, sin embargo, todavía estamos lejos de tener un protocolo de comunicación funcional y resistente para usuarios de alta velocidad y una comunicación automotriz para la computación en niebla. Se pueden usar algoritmos de predicción de movilidad basados en el aprendizaje automático en el diseño de

protocolos de enlace y autenticación, para predecir la ubicación de los usuarios de alta velocidad y analizar sus patrones de movilidad para la computación de niebla. Además de los protocolos de enlace y autenticación para usuarios de alta velocidad, se requiere que el aprovisionamiento del servicio de niebla para aplicaciones IoT sea dinámico y proactivo debido a los rápidos cambios (como conectividad, fluctuaciones de ancho de banda o fallas) en dispositivos móviles y de alta velocidad. Para abordar el aprovisionamiento dinámico y proactivo del servicio de niebla, predecir el comportamiento y la ubicación de los dispositivos IoT y los usuarios de alta velocidad basados en datos históricos o métodos de aprendizaje automático es otra solución potencial que requiere mayor investigación [3].

#### 7.10. SEGURIDAD DEL NODO DE NIEBLA

Los nodos de niebla se colocarán cerca de los usuarios, en ubicaciones como en las estaciones base o enrutadores, o incluso en el extremo de la red en los puntos de acceso WiFi. Esto hace que sea difícil proporcionar seguridad para los nodos de niebla. Los ataques al sitio son más posibles en los nodos de niebla que en los centros de datos en la nube. Una dirección de investigación puede ser diseñar sitios de nodos de niebla seguros, seguros contra daños físicos, atascos, etc. Además, otra dirección puede ser diseñar políticas de control de acceso sólidas para los nodos de niebla, de modo que estén seguros en presencia de usuarios maliciosos en la región. Un punto de partida potencial para el control de acceso en la computación de niebla [3]

#### 7.11. SELECCIÓN DEL SITIO DEL NODO DE NIEBLA

Pocos estudios abordan el problema de selección del sitio del nodo de niebla, que es un problema de diseño para encontrar ubicaciones apropiadas para desplegar nodos. Las estrategias de selección de sitios de nodos de niebla deben considerar la comunicación, el almacenamiento y la computación al mismo tiempo para encontrar una ubicación adecuada (un punto de acceso a la comunicación puede no ser necesariamente un punto de acceso de almacenamiento o de cómputo). Además, el costo también debe ser un factor decisivo en las estrategias de selección del sitio del nodo de niebla; desplegar nodos de niebla en Manhattan puede ser una buena decisión

con respecto a la reducción de la latencia y el ancho de banda, pero puede no ser una buena decisión con respecto a los costos de alquiler. Además, las consideraciones de seguridad del nodo de niebla que se analizan anteriormente en “Seguridad del nodo de niebla” también podrían afectar la decisión de selección del sitio del nodo de niebla [3].

## 7.12. DISEÑO DE SISTEMA DE NIEBLA RESISTENTE

Desde la perspectiva de confiabilidad y disponibilidad, los servicios de niebla y las redes de niebla presentan nuevos desafíos para la red actual y los métodos de suministro de servicios. Para garantizar la disponibilidad y confiabilidad de los servicios de niebla, se necesita un mecanismo coordinado de provisión de servicios que considere tanto la computación de niebla como la de nube. Por ejemplo, si un servicio de niebla necesita algunas funciones para procesar un flujo de datos, proporcionar respuestas adicionales de esas funciones puede mejorar la disponibilidad del servicio. Por otro lado, debido a los recursos informáticos limitados de los nodos de niebla en comparación con los centros de datos en la nube, la asignación de las réplicas de funciones para proporcionar disponibilidad y confiabilidad no es una decisión sencilla. Como una dirección futura, se puede considerar la disponibilidad además de las limitaciones, como la latencia, el rendimiento y la seguridad al diseñar métodos de suministro para servicios de niebla. La mayoría de los artículos en la literatura sobre cómputo de niebla no consideran fallas o fallas en la red de niebla. Otra dirección de investigación es proporcionar diferentes mecanismos de protección y restauración en diferentes capas. Además, la detección, prevención y recuperación de fallas son formas eficientes de mejorar la disponibilidad de los servicios de niebla. Además, los nodos de niebla son más propensos a los ataques de denegación de servicio (DoS), ya que tienen más recursos limitados que los centros de datos en la nube adecuadamente protegidos; además, los nodos de IoT recientemente comprometidos y los sistemas integrados se están convirtiendo en nuevas fuentes de ataques DoS distribuidos. Se podrían utilizar nuevas clases de técnicas de defensa proactiva basadas en el paradigma de defensa del objetivo móvil (a veces denominado mutación / aleatorización de direcciones) para frustrar los ataques DoS. Los investigadores de UC Berkeley recientemente propusieron un marco de computación de

borde resistente, que es un buen punto de partida en la dirección del diseño de un sistema de niebla resistente [3].

### 7.13. FEDERACIÓN DE NIEBLA

Actualmente, no existe un marco o software de federación de niebla (similar al de los esquemas de federación de nube híbrida), que controla y genera recursos de niebla en múltiples dominios operativos. Hay una necesidad de nuevos esquemas para la federación de nodos de niebla, especialmente cuando pertenecen a diferentes dominios operativos. El esquema de federación debe tener en cuenta los modelos de intercambio de recursos para nodos de niebla de diferentes proveedores / operadores. Del mismo modo, se pueden definir nuevos modelos de precios para los recursos de niebla federados. Finalmente, uno puede proponer políticas para nuevos esquemas de intercambio de recursos de niebla (por ejemplo, modelo de intercambio de recursos de computación de niebla P2P) bajo el marco de la federación [3].

### 7.14. COMPUTACIÓN DE NIEBLA P2P

Los modelos actuales de recursos de computación de niebla asumen un modelo simple de cliente-servidor, donde los dispositivos IoT (clientes) usan computación en la nube o computación en la niebla (servidor) para procesar sus solicitudes, mientras que los nodos de niebla también pueden descargar la computación entre ellos o en la nube. Argumentamos que el diseño de un marco completo de recursos punto a punto (P2P) para la computación de niebla es una dirección prometedora. Bajo el modelo de computación de niebla P2P, los nodos de niebla comparten recursos de una manera P2P, donde los nodos de niebla individuales comparten sus recursos (por ejemplo, computación o almacenamiento), sin un tercero intermediario. El modelo de recurso de computación de niebla P2P podría manejar aún más la heterogeneidad y la movilidad de los nodos de niebla (por ejemplo, cuando un nodo de niebla abandona la red P2P). La computación de niebla P2P es la más beneficiosa cuando no hay conectividad a la nube, por ejemplo, cuando hay desastres como inundaciones o terremotos y la conexión a los recursos de la nube se ha ido. El precio de los recursos de niebla P2P es otra dirección de investigación, donde se podrían proponer diferentes métodos de precios e incentivos



para el modelo de intercambio de recursos P2P. La tecnología Blockchain podría ser una opción para realizar un seguimiento de las transacciones de recursos de niebla al diseñar un modelo de precios de recursos de niebla P2P [3].

### 7.15. CONFIANZA Y AUTENTICACIÓN EN SISTEMAS DE NIEBLA HETEROGÉNEOS

Además de la movilidad que se analiza en "Soporte de usuarios de alta velocidad", la heterogeneidad de los nodos de niebla y los dispositivos IoT hace que los protocolos convencionales de confianza y autenticación no sean adecuados para los sistemas de niebla. Además, los nodos de niebla pueden pertenecer a diferentes proveedores y operadores. Por lo tanto, se necesita diseñar nuevos mecanismos de autenticación y confianza para nuevos sistemas de niebla que puedan hacer frente a la heterogeneidad de los nodos de niebla y los dispositivos IoT. Algunos investigadores han comenzado a abordar la heterogeneidad en el diseño de su sistema de niebla [3].

### 7.16. DESCARGA SEGURA DE NIEBLA

Las tareas de descarga entre nodos de niebla pueden incurrir en algunos riesgos de seguridad y privacidad. El riesgo es cuando se descargan las tareas que contienen información crítica para la seguridad y la privacidad. Además, un riesgo de seguridad podría ser cuando un nodo de niebla se sobrecarga (por ejemplo, por las solicitudes enviadas por un usuario malintencionado) y comienza a descargar información crítica de seguridad y privacidad a otros nodos de niebla (que pueden ser accesibles para el usuario malicioso). Una dirección de investigación, por lo tanto, es diseñar e implementar esquemas seguros de descarga y equilibrio de carga. En el se incluye un esfuerzo inicial para la descarga de información sobre privacidad en MEC. Además, el diseño de un mecanismo ligero y eficiente para los receptores de IoT para verificar la corrección e integridad de las tareas descargadas [3].

### 7.17. PAAS PARA LA COMPUTACIÓN DE NIEBLA

No hay implementaciones sólidas de un PaaS para sistemas de niebla, donde los desarrolladores puedan desarrollar fácilmente software a través de niebla, IoT y nube

son algunos de los muy pocos esfuerzos en esta dirección. El desarrollo de un PaaS para la computación en niebla puede facilitar el desarrollo general y la aceptabilidad de la computación en niebla. El futuro PaaS para la computación de niebla debe ocultar la especificación de configuración de niebla (por ejemplo, ubicación de nodos de niebla, su interconexión, su capacidad) para usuarios, suministrar aplicaciones y servicios de manera proactiva y automática con el mínimo esfuerzo de los desarrolladores y admitir diferentes comunicaciones. y protocolos y API a nivel de aplicación. Una vez que este PaaS esté disponible, su diseño modular también podría tenerse en cuenta para que varios complementos para diferentes aplicaciones y servicios de compilación de niebla puedan integrarse fácilmente con el PaaS [3].

#### 7.18. ESTANDARIZACIÓN DE LA COMPUTACIÓN EN NIEBLA

Diferentes equipos de investigación proponen muchas definiciones independientes de niebla (y paradigmas informáticos relacionados con la niebla, como la computación de vanguardia). Las definiciones de cómputo de niebla y sus paradigmas informáticos relacionados no están completamente estandarizadas. Se cree que hay un vacío de investigación en las definiciones y estándares para la computación de niebla y otros paradigmas de computación relacionados con la niebla que deben ser llenados por estándares y definiciones universalmente acordadas. Una vez que se acuerdan las definiciones, los investigadores se vuelven más claros al definir los problemas, y habrá más acuerdo entre los investigadores y la industria sobre estos paradigmas. Organizaciones como OpenFog Consortium y OpenEdge Computing ya están desarrollando estándares y definiciones para la computación de niebla y la computación periférica [3].

#### 7.19. TECNOLOGÍAS DE HARDWARE PARA NIEBLA.

La mayoría de los estudios en el área de la computación de niebla o la computación de borde no hacen uso de nuevas tecnologías de hardware o comunicación, como tecnologías de almacenamiento no volátiles, redes ópticas, fibra inalámbrica (FiWi) o FPGA. El uso de nuevo hardware y tecnologías de comunicación para el diseño de

redes de niebla (por ejemplo, interconexión de niebla a nube) es una dirección que vale la pena explorar [3].

Desafío	Limitación de corriente	Dirección de investigación o solución potencial	Características u objetivos relacionados	Categorías relacionadas
<b>Sistema de niebla SLA</b>	<p>Los SLA no están definidos para sistemas de niebla. Los SLA actuales se definen para la nube.</p> <p>Servicios o infraestructura de red.</p>	<ul style="list-style-type: none"> <li>•Definir SLA nuevo y compatible para sistemas fog.</li> <li>•Diseñar técnicas de gestión de SLA y marco para la computación de fog.</li> <li>•Soporte para SLA de múltiples proveedores o proveedores para sistemas fog.</li> </ul>	QoS, Costo.	Arquitecturas y marcos para fog; control y monitoreo.
<b>Diseño de sistemas fog multiobjetivo</b>	Muchos esquemas (descarga, carga y equilibrio) considere pocos objetivos e ignorar otros objetivos.	•Proponer esquemas que consideren múltiples objetivos (latencia, ancho de banda, energía) simultáneamente (por ejemplo, un esquema eficiente de descarga de tareas que considera ancho de banda, tiempo de espera, disponibilidad, seguridad y energía).	QoS, costo, energía, ancho de banda.	Análisis de recursos y estimación; programación, descarga y carga, balanceo; Bancos de pruebas y experimentos
<b>Diseño de sistemas de fog con</b>	Pocos trabajos consideran el ahorro	•Necesita más estudios sobre el	Ancho de banda.	Bancos de pruebas y experimentos;

<b>reconocimiento de ancho de banda.</b>	de ancho de banda mediante el uso de la computación de niebla, a pesar de que una de las características prometedoras de fog es reducir el ancho de banda de uso en el núcleo.	ahorro de ancho de banda mediante el uso de fog. •Realizar estudios de medición para capturar el uso real del ancho de banda en presencia de fog.		programación, descarga y equilibrio de carga; control y monitoreo; análisis de recursos y estimación; diseño de infraestructura.
<b>Diseño escalable de esquemas fog.</b>	Muchos de los esquemas y algoritmos existentes para fog no se ajustan a su magnitud de las redes IoT.	•Diseñar algoritmos y esquemas escalables para sistemas de fog, por ejemplo, esquema de descarga de tareas en línea que no considere nodos de IoT individuales para la toma de decisiones.  •Verificar la escalabilidad del algoritmo y los esquemas mediante la implementación real.	Escalabilidad.	Provisión de servicios; colocación, programación, descarga y equilibrio de carga: aplicaciones.
<b>Computación de niebla móvil.</b>	La mayoría de la literatura existente supone que los nodos de niebla son fijos o	•Proponga computación de niebla móvil, donde	Movilidad, Gestión	Descubrimiento de recursos; Conceptos y marcos utilizando la niebla; Modelos de

	<p>se centran en la movilidad de los dispositivos IoT. Si los nodos de niebla son móviles, la disponibilidad de recursos, la descarga y el aprovisionamiento de recursos será más difícil.</p>	<p>los nodos de niebla pueden moverse.</p> <ul style="list-style-type: none"> <li>• Esquema para la gestión o federación de nodos de niebla móviles.</li> <li>• Método de aprovisionamiento para servicios de niebla móvil para mantener el servicio siempre disponible para los nodos de IoT.</li> <li>• Diseño de esquemas de descarga y programación de tareas conscientes de la movilidad cuando los nodos de niebla son móviles.</li> </ul>		<p>programación y modelado de datos; Servicio Aprovisionamiento; Seguridad y privacidad; Programación, descarga y equilibrio de carga</p>
<p><b>Monitoreo de recursos de fog.</b></p>	<p>Pocos estudios abordan el monitoreo de los recursos de fog. El monitoreo es más desafiante si varios operadores usan un nodo de fog.</p>	<ul style="list-style-type: none"> <li>• Técnicas de monitoreo de recursos de fog para múltiples operadores.</li> <li>• Software de monitoreo basado en SDN para monitoreo</li> </ul>	<p>Gestión, programabilidad</p>	<p>Control y monitoreo; Software y herramientas</p>

		de recursos y publicidad de recursos.		
<b>Computación de niebla verde.</b>	La mejora del consumo general de energía de fog no se ha estudiado bien (se consideró la descarga de cómputo consciente de la energía, la gestión de la movilidad consciente de la energía y la federación de dispositivos IoT para mejorar consumo de energía).	<ul style="list-style-type: none"> <li>•Uso de recolectores de energía y almacenamiento de baterías para dispositivos y sensores IoT.</li> <li>• Colocación de nodos de fog conscientes de la energía, por ejemplo, cerca de recursos de energía renovable (solar, eólica o vibración)</li> </ul>	Energía	Diseño de infraestructura; Análisis de recursos y estimación
<b>Soporte de usuarios de alta velocidad.</b>	Los protocolos de comunicación actuales no admiten usuarios de alta velocidad.	<ul style="list-style-type: none"> <li>•Desarrollar protocolos de apretón de manos rápidos o sin estado para usuarios de alta velocidad, por ejemplo, usuarios en vehículos o para comunicación automotriz.</li> <li>•Desarrollar algoritmos de predicción de movilidad basados en</li> </ul>	Movilidad, RAS	Arquitecturas y marcos para fog; Provisión de servicios; Descubrimiento de recursos

		el aprendizaje automático.		
<b>Seguridad del nodo de fog</b>	Los nodos de fog normalmente se encuentran cerca de los usuarios, por ejemplo, en las estaciones base, enrutadores o incluso en el extremo de la red, como los puntos de acceso WiFi. Esto hace su seguridad desafiante.	<ul style="list-style-type: none"> <li>•Diseño de nodos de fog físicamente seguros contra ataques al sitio.</li> <li>•Diseñar hardware seguro, seguro contra daños físicos, atascos, etc.</li> <li>•Diseñar políticas sólidas de control de acceso para los nodos de fog.</li> </ul>	Seguridad, heterogeneidad	Seguridad y privacidad; Diseño de infraestructura; Pila de hardware y protocolo
<b>Soporte SDN para fog.</b>	SDN no tiene soporte nativo para fog.	•Mejora y estandarización de SDN (por ejemplo: Interfaz OpenFlow en dirección norte, sur, este-oeste) para casos de uso de fog.	Fundación, programabilidad.	Definición y estándares; Software y herramientas.
<b>Selección del sitio del nodo de fog.</b>	Pocos estudios abordan el problema de selección del sitio del nodo de fog, que es un problema de diseño para encontrar ubicaciones apropiadas para la implementación de nodos.	•Desarrollar estrategias de selección de sitios de nodos de fog que consideren la comunicación, el almacenamiento y la computación (un punto de acceso de comunicación puede	Costo, RAS, QoS, Energía	Diseño de infraestructura; Análisis de recursos y estimación



		<p>no ser un punto de acceso de almacenamiento o computación).</p> <ul style="list-style-type: none"> <li>• Considerar el costo en las estrategias de selección de sitios de nodos de fog (por ejemplo, implementar nodos de fog en Manhattan puede ser una buena decisión con respecto a la latencia y el ancho de banda, pero puede no ser una buena decisión con respecto a los costos de alquiler).</li> </ul>		
<b>Diseño de sistema de fog resistente</b>	<p>Las redes de fog actuales no consideran fallas o fallas en la red. Además, los ataques de denegación de servicio (DoS) son más posibles en los nodos de fog, ya que tienen más recursos limitados que los servidores en la nube.</p>	<ul style="list-style-type: none"> <li>• Detección de fallas, prevención de fallas y recuperación de fallas en redes basadas en fog.</li> <li>• Diseño de sistema de fog resistente a DoS</li> <li>• Diseñe un mecanismo de protección coordinado</li> </ul>	RAS, Seguridad	<p>Control y monitoreo; Diseño de infraestructura; Servicio de Aprovisionamiento; Seguridad y privacidad</p>

		que considere la fog y la nube para garantizar la disponibilidad.		
<b>Federación de fog.</b>	No existe un marco o software de federación de fog similar al de los esquemas de federación de nube híbrida.	<ul style="list-style-type: none"> <li>•Diseñar nuevos esquemas para la federación de nodos de fog, en diferentes dominios operativos.</li> <li>•Diseñar modelos de intercambio de recursos para nodos de fog de diferentes proveedores / operadores.</li> <li>•Definir nuevos modelos de precios para esquemas federados de intercambio de recursos de fog.</li> </ul>	Gestión, programabilidad.	Colocación; Software y herramientas; Descubrimiento de recursos. Provisión de servicios
<b>Computación de fog P2P</b>	Los modelos actuales de recursos de computación de fog suponen un modelo simple de cliente-servidor.	<ul style="list-style-type: none"> <li>•Diseñar un marco completo de recursos P2P para fog que maneje la heterogeneidad y la movilidad de los nodos de fog.</li> <li>•La computación de niebla P2P es</li> </ul>	Fundación, movilidad, heterogeneidad	Conceptos y marcos utilizando fog; Descubrimiento de recursos; Provisión de servicios; Seguridad y privacidad

		<p>beneficiosa cuando no hay conectividad a la nube (por ejemplo, en desastres como inundaciones, terremotos, etc.)</p> <ul style="list-style-type: none"> <li>•Precios de recursos de fog P2P, donde blockchain podría usarse para registrar transacciones de recursos de fog.</li> </ul>		
<b>Confianza y autenticación en sistemas de fog heterogéneos</b>	<p>La heterogeneidad de los nodos de fog y los nodos de IoT hace que los protocolos convencionales de confianza y autenticación no sean adecuados para los sistemas de fog.</p>	<ul style="list-style-type: none"> <li>•Diseñar nuevos mecanismos de autenticación y confianza que puedan hacer frente a la heterogeneidad de los nodos de fog y los nodos de IoT.</li> <li>•Diseñar protocolos de autenticación para nodos de fog de diferentes proveedores / operadores.</li> </ul>	Heterogeneidad, seguridad	<p>Definición y estándares; Seguridad y privacidad; Pila de hardware y protocolo</p>
<b>Descarga segura de fog</b>	<p>La descarga de tareas a los nodos de fog puede generar algunos riesgos de</p>	<ul style="list-style-type: none"> <li>•Diseñar esquemas seguros y privados de descarga y equilibrio de carga.</li> </ul>	Seguridad, QoS	<p>Programación, descarga y equilibrio de carga; Seguridad y privacidad</p>

	seguridad y privacidad.	<ul style="list-style-type: none"> <li>• Un mecanismo para que los receptores verifiquen la corrección e integridad de la tarea descargada.</li> </ul>		
<b>PaaS para computación de niebla</b>	Falta de un PaaS para sistemas de fog, donde los desarrolladores pueden desarrollar fácilmente software a través de fog, IoT y nube.	<ul style="list-style-type: none"> <li>• Desarrollar un PaaS para la computación de niebla, que es transparente para los usuarios y admite diferentes protocolos y API a nivel de comunicación y aplicación.</li> <li>• Desarrollo de complementos para PaaS para diferentes aplicaciones de cómputo de niebla</li> </ul>	programabilidad, gestión	Software y herramientas; Provisión de servicios; Modelos de programación y modelado de datos
<b>Estandarización de la computación de niebla</b>	Se proponen muchas definiciones independientes de fog (y paradigmas informáticos relacionados con fog).	<ul style="list-style-type: none"> <li>• Unánime y universalmente acordado en la definición de la computación de niebla.</li> </ul>	Fundamento.	Definición y estándares.
<b>Tecnologías de hardware para niebla</b>	La mayoría de los estudios no utilizan nuevas tecnologías de comunicación o hardware disponibles.	<ul style="list-style-type: none"> <li>• Uso de nuevas tecnologías de hardware y comunicación, como tecnologías de</li> </ul>	Escalabilidad.	Pila de hardware y protocolo

		almacenamiento no volátiles, redes ópticas y FPGA.		
--	--	--	--	--

*Tabla 6.- Desafíos y futuras direcciones de investigación.*

## CONCLUSIONES

Al estudiar a fondo este paradigma llamado computación en la nube nos hace reflexionar en como ayudará esto a nuestra vida cotidiana, actualmente con el crecimiento de la tecnología y el internet de las cosas, se ha creado una hiperconectividad a la nube, la cual cada minuto recibe cientos de miles de datos, los cuales debe procesar y almacenar, pero entre más dispositivos estén conectados es posible que en un momento la nube no pueda satisfacer las necesidades futuras.

Para satisfacer las futuras necesidades de conectividad se ha desarrollado el concepto de computación en la niebla que surge del mismo concepto de la nube, aun refiriéndonos en el mismo contexto geográfico, la niebla es una parte de la nube más cerca de nosotros, nuestros dispositivos conectados a internet y sensores.

Este nuevo paradigma funciona con una arquitectura sencilla y de bajo consumo energético comparado con los grandes centros de datos de la nube, esta estructura funciona gracias a enrutadores, conmutadores estaciones bases y gateway entre otros, los cuales deben ser distribuidos geográficamente descentralizados para un óptimo funcionamiento, al igual que estos dispositivos existen los nodos de niebla los cuales cumplen una función primordial para una baja latencia y ancho de banda.

En un futuro se esperan diferentes aplicaciones, las cuales están enfocadas principalmente al internet de las cosas, redes de quinta generación y hasta el cuidado de la salud, buscando como principal objetivo mejorar el servicio de la red y no saturar la nube con datos que se pueden procesar de manera local.

Finalmente, la computación en la niebla en una realidad que cada vez está más presente en nuestro entorno, y no precisamente para competir con la nube, si no como una extensión de esta.

## REFERENCIAS

- [1] R. Neware, "Fog Computing Architecture, Applications and Security Issues: A Survey," Preprints, India, 2019.
- [2] R. Mahmud, R. Kotagiri and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," in *Internet of Everything*, Springer, 2018, pp. 103-130.
- [3] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong and J. P. Jue, "survey, All one needs to know about fog computing and related edge computing paradigms: A complete survey," USA, 2018.
- [4] R. K. Naha, L. Gao, S. Garg, D. Georgakopoulos, P. P. Jayaraman, Y. Xiang and R. Ranjan, "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions," IEEE, 2018.
- [5] G. M. C. X. M. E. P. Evangelos Markakis, *Cloud and Fog Computing in 5G Mobile Networks*, United Kingdom: CPI Group (UK), 2017.
- [6] P. Hu, S. Dhelima, H. Ninga and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," ELSEVIER, China, 2017.
- [7] S. Svorobej, P. T. Endo, M. Bendeche, C. Filelis-Papadopoulos, K. M. Giannoutakis, G. A. Gravvanis, D. Tzovaras, J. Byrne and T. Lynn, "Simulating Fog and Edge Computing Scenarios: An Overview and Research Challenges," MPDI, 2019.
- [8] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini and A. Zanni, "A survey on fog computing for the Internet of Things," ELSEVIER, USA, 2019.
- [9] Y. Ai, M. Peng and K. Zhang, "Edge computing technologies for Internet of Things: a primer," ELSEVIER, USA, 2017.

- [10] L. Shu, M. MUKHERJEE, R. MATAM, L. MAGLARAS, M. A. FERRAG, N. CHOUDHURY and V. KUMAR, "Security and Privacy in Fog Computing: Challenges," IEEE, 2017.
- [11] H. F. Atlam, R. J. Walters and G. B. Wills, "Fog Computing and the Internet of Things: A Review," 2018.
- [12] Z. H. Z. Q. a. Q. L. S. Yi, "Fog Computing: Platform and Applications " in Proceedings - 3rd Workshop on Hot Topics in Web Systems and Technologies," HotWeb, Washington, DC, 2015.
- [13] W. Xiang, K. Zheng and X. (. Shen, "5G Mobile Communications," Springer, Cham, Switzerland , 2017.
- [14] A. M. and H. M., "Fog Computing: The Cloud-IoTV/IoE Middleware Paradigm," in IEEE Potentials," *IEEE*, vol. 35, no. 15985113, pp. 40 - 44, 2016.
- [15] B. Flavio, M. Rodolfo, N. Preethi and Z. Jiang, Fog Computing: A Platform for Internet of Things and Analytics, Springer, Cham, 2014.
- [16] H. Kirak, L. David and R. Umakishore, Mobile Fog: A Programming Model for Large–ScaleApplications on the Internet of Things, Atlanta, Georgia, USA, pp. 15 - 20.
- [17] J. Oueis, E. C. Strinati, S. Sardellitti and S. Barbarossa, "Small Cell Clustering for Efficient Distributed Fog Computing: A Multi-User Case," in *IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Boston, MA, 2015.
- [18] A. Banafa, "OpenMind," 2015 Julio 27. [Online]. Available: <https://www.bbvaopenmind.com/tecnologia/mundo-digital/internet-de-las-cosas-y-computacion-de-la-niebla/>. [Accessed 54 Septiembre 2019].
- [19] H. Chourabi, "Understanding Smart Cities: An Integrative Framework," in *45th Hawaii International Conference on System Sciences*, Maui, HI, 2012.



- [20] R. Vilalta, "TelcoFog: A Unified Flexible Fog and Cloud Computing Architecture for 5G Networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 36-43, 2017.
- [21] S. Rick, P. Carol and C. Julie, "Application Performance Management (APM) in the Digital Enterprise: Managing Applications for Cloud, Mobile, IoT and eBusiness," United States, Morgan Kaufmann, 2017, pp. 41-52.
- [22] S. Mondal, G. Das and E. Wong, "A Novel Cost Optimization Framework for Multi-Cloudlet Environment over Optical Access Networks," in *IEEE Global Communications Conference*, Singapore, GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1-7.
- [23] Q. Fan and N. Ansari, "Cost Aware cloudlet Placement for big data processing at the edge," in *7 IEEE International Conference on Communications (ICC)*, Paris, 2017.
- [24] Y. Shih, W. Chung, A. Pang, T. Chiu and H. Wei, "Enabling Low-Latency Applications in Fog-Radio Access Networks," in *IEEE*, IEEE, 2017, pp. 52-58.
- [25] F. Jalali, K. Hinton, R. Ayre, T. Alpcan and R. S. Tucker, "Fog Computing May Help to Save Energy in Cloud Computing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1728-1739, 2016.
- [26] M. S. H. Nazmudeen, A. T. Wan and S. M. Buhari, "Improved throughput for Power Line Communication (PLC) for smart meters using fog computing based data aggregation approach," in *IEEE International Smart Cities Conference (ISC2)*, Trento, 2016.
- [27] M. R. Mahmud, A. Mahbuba, R. Md. Abdur, M. H. Mohammad, A. Abdulhameed and A. Majed, "Maximizing quality of experience through context-aware mobile application scheduling in cloudlet infrastructure," Wiley, 2016.
- [28] L. Gu, D. Zeng, S. Guo, A. Barnawi and Y. Xiang, "Cost Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical

- System," in *IEEE Transactions on Emerging Topics in Computing*, IEEE, 2017, pp. 108-119.
- [29] S. Yan, M. Peng and W. Wang, "User access mode selection in fog computing based radio access networks," in *IEEE International Conference on Communications (ICC)*, Kuala Lumpur, 2016.
- [30] M. Aazam and E. Huh, "Fog Computing and Smart Gateway Based Communication for Cloud of Things," in *International Conference on Future Internet of Things and Cloud*, Barcelona, 2014.
- [31] W. Lee, K. Nam, H. Roh and S. Kim, "A gateway based fog computing architecture for wireless sensors and actuator networks," in *8th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, 2016.
- [32] M. Aazam, M. St-Hilaire, C. Lung and I. Lambadaris, "PRE-Fog: IoT trace based probabilistic resource estimation at Fog," in *13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2016, 2016.
- [33] D. Zeng, L. Gu, S. Guo, Z. Cheng and S. Yu, "Joint Optimization of Task Scheduling and Image Placement in Fog Computing Supported Software-Defined Embedded System," *IEEE Transactions on Computers*, vol. 65, no. 12, pp. 702-3712, 2016.
- [34] K. Intharawijitr, K. Iida and H. Koga, "Analysis of fog model considering computing and communication latency in 5G cellular networks," in *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, Sydney, NSW, 2016.
- [35] H. Shi, N. Chen and R. Deters, "Combining Mobile and Fog Computing: Using CoAP to Link Mobile Device Clouds with Fog Computing," in *IEEE International Conference on Data Science and Data Intensive Systems*, Sydney, NSW, 2015.

- [36] N. K. Giang, M. Blackstock, R. Lea and V. C. M. Leung, "5th International Conference on the Internet of Things (IOT)," in *Developing IoT applications in the Fog: A Distributed Dataflow approach*, Seoul, 2015.
- [37] J. Oueis, E. C. Strinati and S. Barbarossa, "The Fog Balancing: Load Distribution for Small Cell Cloud Computing," in *IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, 2015.
- [38] M. A. Hassan, M. Xiao, Q. Wei and S. Chen, "Help your mobile applications with fog computing," in *12th Annual IEEE International Conference on Sensing, Communication, and Networking - Workshops (SECON Workshops)*, Seattle, WA, 2015.
- [39] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in *Federated Conference on Computer Science and Information Systems*, Warsaw, 2014.
- [40] A. M. Elmisery, S. Rho and D. Botvich, "A Fog Based Middleware for Automated Compliance With OECD Privacy Principles in Internet of Healthcare Things," *IEEE Access*, vol. 4, pp. 8418-8441, 2016.
- [41] B. Paolo, B. Javier, C. Antonio, K. D. Sajal, F. Luca and Z. Alessandro, "A survey on fog computing for the Internet of Things," *Pervasive and Mobile Computing*, vol. 52, pp. 71- 99, 2019.