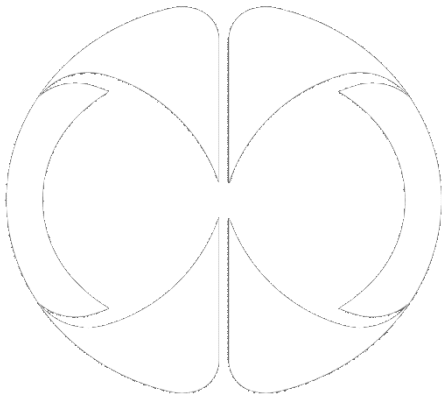

Fundación Universitaria
SAN MATEO

FACULTAD DE INGENIERIAS

INGENIERIA EN TELECOMUNICACIONES

I.

ANALISIS GENERAL DEL ENFOQUE IOT EN REDES

TRABAJO DE GRADO MODALIDAD DE OPCIÓN DE GRADO

II.

DIRECTOR (A)

HERNAN DARIO JIMENEZ JIMENEZ

BOGOTA D.C

2019

BRAYAN ALEXANDER HERNANDEZ
DIANA PAOLA ORTIZ GALEANO

NOTA DE SALVEDAD DE RESPONSABILIDAD INSTITUCIONAL

"La Fundación Universitaria San Mateo NO se hace responsable de los conceptos emitidos en el presente documento, el departamento de investigaciones velará por el rigor metodológico de la investigación".

CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

DEDICATORIA

AGRADECIMIENTOS

ABREVIATURAS

IOT (INTERNET OF THINGS.)

IDS (SISTEMA DE DETECCIÓN DE INTRUSOS.)

IPS (SISTEMA DE PREVENCIÓN DE INTRUSOS.)

ISP (PROVIDE SERVICE INTERNET.)

SGSI (Sistema de gestión de seguridad de la información.)

UIT (unión internacional de telecomunicaciones.)

DDOS(denegación de servicio distribuido)

RFID (Identificación por Radiofrecuencia.)

UPNP (Universal plug and play)

IANA (internet assigned Numbers authority)

TMN(Telecomunication Network Management)

PDU (unidad del protocolo de datos)

PBM (Policy Based Management)

WBEM (Web Based Enterprise Management)

LAN (local area network)

M2M (machine to machine)

RESUMEN

PALABRAS CLAVE: IoT, malware, ataque cibernetico, seguridad informatica, IPV4, IPV6, Integridad, blockchain, vulnerabilidad, internet, smart city, smart home, intrusión,bots,bonet,RFID,m2m,wsn.

En el transcurso del documento encontraremos una breve reseña del nacimiento de IOT , en la investigación se conoce el origen de este término aparece en el año de 1999 dado en una conferencia, donde después la ITU en el año del 2005 divulga acerca de esta nueva tecnología cuya diferencia frente a las demás redes que eran solo computadoras, es conectar cosas y realización, ejecución de redes dinámicas con conectividad desde cualquier momento y lugar, generando facilidades en todos los campos desde la medicina, ciudades, agricultura, entre otros, con uso de tecnologías basadas en radiofrecuencia como es el mismo RFID,redes inalámbricas de sensores como las WSN, uso de redes de área personal, redes wlan en conjunto con tecnologias como el uso de la nube,big data, desde luego la cantidad de dispositivos aumenta, así que de tal modo aparece el protocolo ipv6 con 128 bits a diferencia de ipv4 que carece de 32 bits, permitiendo así lograr más conectividad de dispositivos en las redes y hacia internet todo esto administrado por IANA, encargada de la coordinación mundial de los sistemas de direccionamiento del protocolo de internet.

Dado a conocer una generalización de lo que conforma IOT, hablaremos de nuestro enfoque del estudio, el cual es la privacidad de la seguridad bajo la aplicación de esta tecnología, en búsqueda de garantizar que los datos que viajan por estas redes y distintas topologías y clasificación de estas se salvaguarde la información, y evadir que esta no sea alterada para evitar la violación de la integridad en los mismos datos o información, de técnicas de ataque y vulnerabilidades en las redes , o directamente al infiltrando al usuario mediante ingeniería social, entre otros aspectos, que pueden generar riesgos en el uso del hogar y ciudades inteligentes.

Para ello se plantean soluciones técnicas y de mediación del uso de esta tecnología al ser consumible para el usuario, generando así una conciencia en el mismo usuario al instante de comprar u observar una cosa orientada a conexión teniendo en cuenta el tipo de información privada que manipularan estos dispositivos entre las redes ya sea de uso hogar o corporativo, donde el documento x.800 de la ITU en conjunto con la CCITT, en búsqueda de soluciones de seguridad de modelos abiertos nombra aspectos a tener en cuenta como un control de acceso, la responsabilidad del administrador como el manipulador de la información generando así una aplicación del no repudio, clasificación de

amenazas, modelos de autenticación, implementación de políticas, de tal modo que con estos ítems a tener en cuenta podemos brindar un nivel mayor de seguridad de nuestras redes, ya que el ingreso de IOT en las redes genera recolección de la información ,espacio de control del usuario y espacio de conocimiento del usuario, para solución de la privacidad de manera técnica dentro de la red se dan a partir de manejos como los IDS e IPS (sistemas detector de intrusos, sistema preventivo de intrusos) brindando no accesos a no autorizados, recopilación de registros de tráfico y consumo dentro de la red, al igual que la aplicación de firewall, métodos de cifrado robustos en el enrutamiento, identificación de dispositivos mediante patrones; un término a tratar en la actualidad y que servirá para un análisis de fondo y a futuro de posibles ataques es la seguridad predictiva encargada de análisis de vulnerabilidades constante en todos los aspectos para el presente y el futuro de la seguridad en enfoque a las tecnologías, donde se incluyen estudios estocásticos, psicológicos y de disuasión, en el ser humano frente a sus tomas de decisiones, puesto como lo nombrábamos la seguridad no solo es fiable de manera técnica sino además el usuario se comporta como (backdoor) dentro del modelado de seguridad en una red, siendo de los más efectivos puesto que la falta de capacitación y comportamientos del mismo usuario frente a la interacción con las políticas de seguridad establecidas aplicando el método estocástico para obtención de resultados.

Volviendo a la parte técnica para el aseguramiento de la integridad de la informática, se genera la aplicación del lenguaje de programación utilizado para administración sistematizada de monedas virtuales como el bitcoin, llamado "blockchain", el cual genera un nivel mayor de seguridad puesto a su manejo y administración del mismo de las transacciones, métodos de autenticación, comunicaciones descentralizadas, primordialmente caracterizado por su manejo de bloques y secuencias de cadena de manejo de las transacciones, de tal modo indicando que es una buena apuesta lo que ofrece blockchain a nivel de seguridad para el IOT.

Podríamos indicar que la cantidad de elementos cosas interconectados en las redes al ser aumentados van en paralelo con el incremento del tráfico a nivel global para ello se requiere de marcos legales que apunten a aspectos jurídicos o de retención de cuentas frente a un mal manejo, intrusión, alteración, entre otros que afecten o vulneren la integridad de la información, que son dirigidos como leyes y estándares globales tales como documentos realizados por ITU,leyes nacionales de acuerdo a cada país, ley de habeas data, estándares ISO 27000,27001,entre otras.

ABSTRACT

KEY WORDS: iot, malware, cyber attack, computer security, IPV4, IPV6, Integrity, blockchain, vulnerability, internet, smart city, smart home, intrusion, bots, bonet, RFID, m2m, wsn.

In the course of the document we will find a brief review of the birth of IOT that in the research is given that this term appears in the year 1999 given in a conference, where after the ITU in the year 2005 discloses about this new technology whose difference compared to the other networks that were only computers, it is connecting things and making, executing dynamic networks with connectivity from any time and place, generating facilities in all fields from medicine, cities, agriculture, among others, with the use of technology based in radiofrequency as it is the same RFID, wireless networks of sensors as the WSN, use of personal area networks, wlan networks in conjunction with technologies such as the use of the cloud, big data, of course the number of devices increases, so such a way appears the protocol ipv6 with 128 bits unlike ipv4 that lacks 32 bits, thus allowing to achieve more connectivity of devices in the and to the internet all this managed by IANA, in charge of the global coordination of the Internet protocol addressing systems.

Given a generalization of what makes up IOT, we will discuss our approach to the study, which is the privacy of security under the application of this technology, in search of ensuring that the data traveling through these networks and different topologies and classification of these is safeguarded the information, and evade that this is not altered to avoid the violation of integrity in the same data or information, attack techniques and vulnerabilities in the networks, or directly by infiltrating the user through social engineering, among others aspects, which can generate risks in the use of the home and smart cities.

To do this, technical and mediation solutions are proposed for the use of this technology as it is consumable for the user, generating an awareness in the same user when buying or observing a connection-oriented thing, taking into account the type of private information that will be manipulated. these devices between the networks, whether for home or corporate use, where the ITU document x.800 in conjunction with the CCITT, in search of security solutions of open models, names aspects to be taken into account as an access control, the responsibility of the administrator as the manipulator of information thus generating an application of non-repudiation, classification of threats, authentication models, policy implementation, so that with these items to be taken into account we can provide a higher level of security of our networks , since the income of IOT in the networks generates data collection, user control space and space of knowledge of the user, for solution of the privacy of technical way within the network they are given from

managements like the IDS and IPS (systems detector of intruders, system preventive of intruders) providing not accesses to not authorized, compilation of registers of traffic and consumption within the network, like the firewall application, robust encryption methods in routing, identification of devices through patterns; a term to be dealt with at present and that will serve for a thorough and future analysis of possible attacks is the predictive security in charge of vulnerability analysis in all aspects for the present and the future of security in approach to technologies, where stochastic, psychological and deterrent studies are included in the human being in front of his decision making, since as we named it, security is not only technically reliable but also the user behaves as (backdoor) within the safety modeling in a network, being of the most effective since the lack of training and behavior of the same user in front of the interaction with the security policies established by applying the stochastic method for obtaining results.

Returning to the technical part for the assurance of the integrity of the computer, the application of the programming language used for systematized management of virtual currencies such as bitcoin is generated, called "blockchain", which generates a higher level of security placed at its management and administration of transactions, authentication methods, decentralized communications, primarily characterized by its handling of blocks and chain sequences of transaction management, thereby indicating that it is a good bet what blockchain offers at the security level for the IOT.

We could indicate that the amount of things interconnected in the networks when increased increases in parallel with the increase in global traffic. For this, legal frameworks that point to legal aspects or retention of accounts in the face of mismanagement, intrusion are required. alteration, among others that affect or violate the integrity of the information, which are addressed as laws and global standards such as documents made by ITU, national laws according to each country, habeas data law, ISO standards 27000,27001, among others.

INTRODUCCIÓN

En la actualidad y el futuro de cosas conectados a internet en incremento al igual que con los modos de acceso, implementación del protocolo ipv6, entre otros, esto a mediados del 2009 empieza a ser público el termino Internet de las cosas, siendo primero implementado ipv6, el cual nacía con el objetivo de permitir conectar más nodos, puesto que ipv4 genera conectividad de 4,294,967,296 direcciones compuestas de 32 bits e ipv6 compuesta de 128 bits generando alrededor de 4.3 billones de direcciones permitiendo el acceso de más nodos, nuevos modos de redes a través de la utilización de medios inalámbricos conocidos desde su publicación por el IEEE como el 802.15, 802.11,802.3,802.15.4 .

Podríamos albergar e indicar que, de acuerdo con todos los medios de acceso para la interconexión de las cosas frente a internet, es una comodidad y revolución en la humanidad con la implementación de cosas en todos los campos posibles de producción, Smart city, Smart home, agricultura, medicina, etc.

Frente a las implementaciones de IOT y sus diferentes medios de red acceso, asimismo se produce el aumento de la ciberdelincuencia intervenida a partir de diferentes métodos que pueden alterar la seguridad de la información de los datos, donde en este enfoque se analiza en el sector de la integridad de los datos en búsqueda de soluciones en protección del mismo, en búsqueda de varios métodos que satisfagan un nivel moderado de protección de la integridad de los datos de todos los nodos persona, cosa y su aplicación en los distintos campos donde el ejemplo mas permisivo seria en el uso de la medicina, ciudades inteligentes y casas inteligentes, las técnicas que se aplican son desde seguridad en las redes hasta análisis de la interactividad del usuario con el dispositivo IOT Mediante el uso de sensores, wifi, bluetooth, entre otros.

Para la satisfacción de una posible protección de la integridad de la información se efectúa la aplicación de solución en la confiablidad de los IDS, IPS en las infraestructuras de redes, la creación de entablación de políticas de uso, análisis de uso de las interacciones de la ciudad inteligente y de cómo afecta una urbanización social referente a la privacidad del usuario, utilización de términos y análisis de posibles soluciones mediante la seguridad predictiva.

CAPITULO I

DESCRIPCIÓN DEL PROYECTO

El proyecto se elabora para estudiar las vulnerabilidades a nivel de privacidad que presenta el Internet de las cosas (IoT[1]) en la busqueda de violación de los datos, en varios campos y cotidianidades. Con el objetivo de buscar soluciones de seguridad cibernética en el IoT, puesto que es unos de los problemas más grandes que se presentan con las implementaciones del mismo en la actualidad.

III. Presentación del problema de investigación

¿Cómo se puede garantizar la privacidad de seguridad de los datos mediante la busqueda de tecnicas informaticas y enfocadas al IOT?

IV. Justificación

En la actualidad y a medida de la evolución de la tecnología la cantidad de cosas estarán interconectados hacia internet vista desde a la accesibilidad en un clic, las smart city, el apoyo de dispositivos electrónicos en hospitales, entre otros, donde de manera paralela y exponencial avanzan las redes para soportar estas cosas para brindar eficiencia y accesibilidad frente a una calidad y servicio.

Por lo tanto el tráfico en estas redes es exponencial, donde para lo cual desde sus surgimientos e implementaciones del IoT ha facilitado más las tareas al ser humano, donde uno de los mayores problemas mundiales es que estos tipos de sistemas han sido abruptamente hackeados, los atacantes informáticos e intrusos realizan la obtención de datos por fuga o vulnerabilidades del sistema IoT cuyo papel es encontrar información del tráfico que circula desde el elemento IoT hasta el hotspot y el destino de este, cuyo resultado de datos obtenidos más allá de los mismos datos del IoT, es el muestreo de un diseño y dispositivos conectados en una red que puede ser de carácter corporativa u hogar, donde luego en lo posible el atacante propenderá al análisis de todas las máquinas de la red en busca de vulnerabilidades de cada una para un mal trato de la información e intrusión en la red, generando asi una violación de

privacidad,entre otros aspectos, ya sea porque el elemento IoT conectado a la red tenía sus credenciales por defecto y por allí se ingresó u otros tipos de acceso mediante técnicas de intrusión famosos en el IoT,tal como el DDos (denegación de servicio distribuido), encargado de saturar el elemento con el propósito de obtención de algún dato, caída del servicio dentro de la red, para ingreso a la misma, entre otros como el uso de los bots y bonet en crecimiento.

Por lo tanto lo que se quiere con la investigación es mejorar y mitigar los tipos de acceso de intrusos informáticos en los elementos IoT debido a que es una gran necesidad con gran demanda puesto que la información personal como de grandes o pequeñas compañías y demas ambientes se ve expuesta en internet por los tipos de conexión comunicaciones de máquina- máquina máquina-persona.

V. Objetivos

A. *Objetivo General*

- Identificar maneras o soluciones para garantizar la integridad de la información en el IoT, para la proposición de soluciones y sistemas que sean seguros y poco vulnerables para los cracker informáticos.

B. *Objetivos Específicos*

- Analizar las vulnerabilidades en la privacidad en conexiones del tipo IoT.
- Estudiar el comportamiento de una comunicación IoT.
- Generar busquedas de tecnicas informaticas u otras que permitan la integridad de los datos.

CAPITULO II

MARCO TEÓRICO

Internet de las cosas, considerado como una infraestructura global de la información por medio de la cual permite ofrecer servicios de interconexión a objetos sea físico o virtual, aprovechando la evolución de la tecnología para el procesamiento de información y la comunicación, para ser aplicado en cualquier entorno.

Los diferentes significados que tiene IoT desde que se conoció este término, fue referenciado con varias definiciones tanto para la Comisión de la Unión Europea, como para Unión Internacional de Telecomunicaciones (ITU), en este texto se puede encontrar que la IoT es una arquitectura que permite compartir la información entre objetos o acerca de las personas a través de una red.

VI. Antecedentes de la investigación

Historia de IoT

En 1926 Nikola Tesla preparo las bases de las comunicaciones, después en el año 1990 Berners-Lee creo HTTP estas son las bases donde posteriormente en el año 1999 Kevin Ashton Fue la persona que utilizo por primera vez la expresión de IoT en una conferencia, desde entonces comenzó a ser normal referirse al sistema de conexión de cosas a internet.

Kevin Asthon Trabajaba en procter & Gamble (P&G) tenía 28 años en ese momento estaba en problemas porque los productos que manejaba no estaban disponibles en las tiendas, se dio cuenta de cuál era el problema de información, por lo tanto se le ocurrió una idea de colocar sensores a los productos para saber cuándo dejaran de estar en stock, el trato de convencer a P&G para poder implementar la idea que tenía.

Asthon asegura que "entendió que la palabra "internet" podría atraer la atención de esta compañía porque en 1998 los gerentes pensaban que la red era lo más importante y buscaban nuevos proyectos. después la palabra "cosas" se comenzó a usar por la idea de empotrar las computadoras en las mesas y cada vez los equipos llegaban más económicos y más pequeños, la idea era confusa pero era lo suficiente para que comenzara a investigar sobre Internet of things".

En 2005 ITU (International Telecommunications Union) realizo el primer estudio sobre el tema, ellos afirmaron lo siguiente "Una nueva dimensión se ha agregado al mundo de las tecnologías de información y la comunicación (TIC): a

cualquier hora, en cualquier lugar, ahora vamos a tener conectividad para cualquier cosa. Las conexiones se multiplican y crearán una nueva red dinámica de redes con redes, una Internet de las Cosas". (Paniagua, 2012)

En el año 2008 un grupo de empresas crearon una alianza para promover el uso de protocolos de internet de objetos inteligentes comenzaron a trabajar en ello para que se hiciera realidad esta idea. La Alliance IPSO tiene empresas involucradas actualmente como Google, Bosch, Motorola, Toshiba. etc.. primero comenzaron con el proyecto de desarrollo del protocolo IPV6.

En el año 2009 comenzó a ser más escuchada esa palabra IoT, en 2011 fue lanzado como tal el protocolo IPV6 y otros fabricantes anunciaron sus proyectos, después se inició la adopción de estándares para IoT a escala global.

Definición de IoT

El paradigma internet of things será considerado en su ámbito de desarrollo como la cuarta revolución industrial ,ya que actuará de cierta manera en campos como la industria y automatización,transporte,salud,ciudades inteligentes,casas inteligentes y actividades de comunidad.

El IoT es la interconexión en red de todos los objetos que se encuentran equipados con algún tipo de inteligencia, la IoT es una verdadera evolución por su interconectividad dando manejo de la información y servicios inteligentes (Silvestre, 2016) afirma:

IoT ofrece grandes oportunidades en diferentes campos, mejorando continuamente la gestión y dando cambio radical en la vida cotidiana ofreciendo nuevas oportunidades en los datos y otros servicios, se puede explorar nuevos modelos de negocio por medio de los dispositivos interconectados.

El avance que ha tenido la IoT y el crecimiento exponencial de los dispositivos electrónicos con los cuales se puede vincular al Internet de las cosas, ha evolucionado cada vez más generando un mayor consumo de estos productos logrando una demanda mayor para la implementación de aplicaciones que permitan realizar trabajos sin mayor esfuerzo.

El IoT pese a generar una gran facilidad de manejo en objetos a distancia, genera que cada uno de los dispositivos deba tener unos requerimientos tecnológicos e infraestructura, para implementar un diseño de redes más especializado y evaluar los costos de tal implementación.

La IoT y el crecimiento exponencial de los dispositivos electrónicos, ha evolucionado cada vez más generando un mayor consumo de estos productos logrando una demanda mayor para la implementación de aplicaciones que permitan realizar trabajos sin mayor esfuerzo.

A continuacion se nombran algunas soluciones implementadas del IOT

- En el hogar permitirá darle órdenes a cada uno de los objetos configurados para realizar acciones predeterminadas.
- En cuanto al sector de la salud permitirá mejorar la calidad de vida, y mejora de los procedimientos médicos ya que permitirá monitorear con más precisión los síntomas y el estado de salud de cada uno de los pacientes.
- En la agricultura se puede reflejar el siguiente paso para el área rural ya que permitirá tener un control más detallado de las condiciones climatológicas y de los cultivos.
- En la parte de industria y comercio la implementación del IoT aumentara la capacidad de control en seguridad, calidad y producción.

No todas las cosas son buenas en la implementación de internet de las cosas ya que esta tecnologías genera un consumo más alto de energía causando que a futuro esto pueda ser un problema de alta demanda de energía teniendo así que implementar distintos medios de aumento de energía.

V. Bases teoricas o fundamentales conceptuales

Características de IoT

IoT ha aumentado en la capacidad de transmisión y procesamiento, anteriormente en la década del 2000 comenzó la propuesta de generar la tecnología necesaria para que IoT hoy en día sea una realidad avanzada, teniendo en cuenta el ahorro energético, también los costos que este con lleva para que sean asequibles para cualquier persona.

A continuación se observara las Tecnologías que contribuyen al desarrollo de IoT en la Tabla.

Tecnologías que Contribuyen directamente al desarrollo de Internet de las Cosas	*Tecnologías que pueden llegar a adicionar valor a Internet de las Cosas*
Interfaces máquina-máquina (M2M) y protocolos de comunicación electrónica	Etiquetado Geográfico
Microcontroladores	Biometría
Comunicación inalámbrica	Máquinas de Visión
Tecnología RFID	Robótica
Tecnología de almacenamiento de energía	Realidad aumentada
Sensores	Escenarios paralelos
Actuadores	Tele presencia
Software	Interfaces tangibles
Tecnología de localización	Tecnologías limpias

Tabla 1. Tecnologías de internet de las cosas.

IoT nació de ciertas tecnologías según afirma (Sosa, 2014) "Radiofrecuencia (RFID) y de las redes inalámbricas de sensores (WSN). Las WSN han sido preferidas en estudios e interacción con el ambiente y situaciones de emergencias y desastres. RFID ha sido concebida como una herramienta ligada a las cadenas de abastecimiento de diferentes productos. Las primeras hacen uso de capacidades limitadas de procesamiento, almacenamiento, transmisión y agregación de Tecnologías que Contribuyen directamente al desarrollo de Internet de las Cosas." (P.4-8).

Los RFID son dispositivos pequeños los cuales pueden ser incorporados a cualquier cosa, existiendo mucha variedad de dispositivos con diferentes capacidades de comunicación y computo, dependiendo el campo donde se requiera utilizar.

los avances de los sistemas Micro-eléctrico-Mecánicos (MEMS) y la computación en la nube, servicios Web, tecnología de sensores RFID (Radio Frecuency-ID) y UPnP (Universal Plug and Play) estas han surgido para la nueva era de IoT.

Se puede observar, analizar y comparar las diferentes arquitecturas que conforman la IoT. Se aclara que la estandarización es un proceso en desarrollo y los principales aportes que destacan la IEEE (Institute of Electrical and

Electronics Engineers), 802.15 y el protocolo 802.15.4 se encarga de permitir la comunicación con bajas tasas de transmisión para trabajar con dispositivos de bajo costo y recursos limitados.

Protocolos

IPV4 – IPV6

Los protocolos IP van de la mano con todo el proceso de interconectividad no solo a personas sino también a objetos esto significa que "Actualmente la IANA (Internet Assigned Numbers Authority) es responsable de la coordinación global de los sistemas de direccionamiento del Protocolo de Internet, así como los Números de Sistemas Autónomos utilizados para enrutar el tráfico de Internet, hoy en día existen dos tipos de direcciones del Protocolo de Internet (IP) en uso activo: IP versión 4 (IPv4) e IP versión 6 (IPv6). IPv4 se desplegó inicialmente el 1 de enero de 1983 y sigue siendo la versión más utilizada. Las direcciones IPv4 son números de 32 bits, la implementación del protocolo IPv6 comenzó en 1999, las direcciones IPv6 son números de 128 bits lo que aumenta varias veces su capacidad de la red, las direcciones IPv4 e IPv6 se asignan generalmente de una manera jerárquica, a los usuarios se les asignan las direcciones IP de los proveedores de servicios de Internet (ISP). Los ISPs obtienen la asignación de direcciones IP a partir de un registro local de Internet (LIR) o Registro Nacional de Internet (RNI), o de su adecuado Registro Regional de Internet (RIR), en la Figura 3-3 se observa el tipo de RIR según la zona de cobertura." (garcia, 2014) Pp 29.

Hoy en día las direcciones IPV4 son insuficientes para satisfacer la demanda puesto que está limitado a 4.3 mil millones de direcciones, la dirección IPV4 es un número formado por 4 octetos dando un valor de 32 bits, cada día los usuarios incrementan en el uso de internet, ahora que llega el sistema de interconexión de objetos,se requiere de mayor asignación de direcciones IP, para ello se implementa el protocolo de direccionamiento IPV6 formada por 128 bits, cuenta con mayor seguridad y espacio de direccionamiento y movilidad, además mejora la compatibilidad del servicio y su infraestructura, ya que genera un enrutamiento eficaz y autoconfiguración.

IPV6 ahorra el procesamiento y ancho de banda, tienen una etiqueta llamada (flow label) esta permite enviar información respecto a la calidad del servicio, genera a los usuarios calidad de acuerdo a sus necesidades. Existe diferencias entre la versión 4 y 6 como: ampliación del tamaño de la dirección, privacidad y autenticación para generar integridad en los datos, estos dos protocolos deben realizar una integración utilizara dos técnicas, una es DUAL STACK y DTTS.

DUAL STACK: es una técnica de integración donde el nodo tiene conectividad para los dos protocolos IPV4 e IPV6, es recomendada para admitir ambos protocolos, cada nodo tendrá la configuración de dos stacks.

DTTS (Dynmic Tunneling Technique): es una técnica de tunelizacion donde se puede implementar la infraestructura de reenvió de IPV6 mientras IPV4 será la base.

Como tal los próximos desarrollos de aplicaciones y servicios serán implementados con el protocolo IPV6, por eso Internet de las cosas necesita de seguridad en la información por los grandes volúmenes de información que manejan y el protocolo IPV6 proporciona una capa de seguridad en la red, este proceso se realiza por medio de IPsec el cual define dos servicios de protocolo de seguridad de encapsulado tales como: ESP (encargado de proporcionar confidencialidad, protección, autenticaciones) y la cabecera de autenticación AH (proporciona autenticación en el origen de los datos y protección de reproducción).

Bajo los estandares del ieee 802.15 y 802.15.4 se puede encontrar diferentes propuestas y protocolos de la capa de aplicación que corre sobre UDP permitiendo conectar dispositivos con recursos limitados a través de la Web, el protocolo RPL (IPv6 Routing Protocol for Lower and Lossy Networks), protocolo de capa de red que permite trabajar los dispositivos limitados o el 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) existe más organizaciones que destacan muchos protocolos como SOAP (Simple Object Access Protocol) que define como los objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.etc.

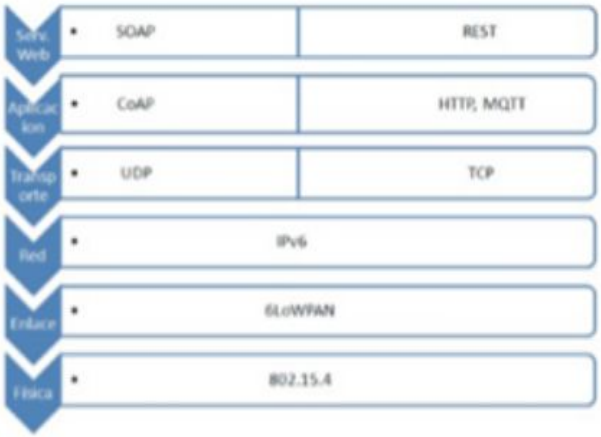

fig 1. stacks de protocolos de la arquitectura IOT

802.15.4 Estándar definido como acceso al medio, permite trabajar con recursos limitados, consumo eficiente de energía y emplea tasas de transmisión baja, dentro de este protocolo se destaca la comunicación ZigBee y tecnología de sensores RFID, también en el área de capa de enlace se encuentra el estándar 6LoWPAN, permite emplear 802.15.4

a IPV6, siendo este el único estándar que tiene una infraestructura de red existente permitiendo la asignación de Ip sin ninguna limitación.

También se puede conocer que funcionamiento tienen en la capa de aplicación los protocolos como CoAP, HTTP y MQTT y otros conocidos FTP, SMTP y JMS, en conclusión se puede ver todos los factores que benefician la arquitectura, permitiendo resolver el problema en sectores específicos y en las intercomunicaciones de objetos por medio de protocolos de internet estandarizados.

De Acuerdo a la afirmación del autor(a) Dana Rodríguez González del artículo, la implementación de gestión de IoT se divide en cuatro grupos como:

SNMP (Simple Network Management Protocol) para gestión de este protocolo deben suplir las limitantes, en caso de no ser así no serán implementadas de forma eficaz para gestionar la IoT las limitantes de este protocolo se encuentran en RFC35126, por ello se deben realizar modificaciones, tales como: gestionar elementos instalando un agente por cada dispositivo, gestor local en cada Gateway y remoto en la infraestructura de red IP existente.

Las modificaciones para este protocolo serán:

Emplear el broadcast para transmisión del mensaje y configuración de los dispositivos ahorrando potencia en caso de que se gestionen dispositivos similares.

Incorporar un GETREquest PDU y StopGETRequest PDU de forma periódica, encargada de optimizar la energía.

Comprimir el mensaje SNMP para igualmente reducir el consumo de energía.

TMN (Telecomunication Network Management).

Permite combinar la robustez de CMIP; es un protocolo que define la información entre aplicaciones de gestión con la interoperabilidad de CORBA; conocido como un framework encargado de entrar en el grupo de sistema de gestión, estos sistemas aportan modularidad, abstracción y reutilización del software.

WBEM (Web Based Enterprise Management)

Es una iniciativa que provee un conjunto de estándares y tecnologías enfocados en la gestión de internet unificando los sistemas de gestión de redes, usuarios y aplicaciones. Tiene como componente fundamental llamado (WBEM-Client) siendo intermediario entre el gestor y el dispositivo, la ventaja es que obtiene la información a partir de una comunicación directa con el CIMOM (pieza clave del WBEM-Server) empleando mensajes. Por otro lado el WBEM-server permite ocultar los detalles de comunicación del gestor, los proveedores, adicionalmente enruta la información de los objetos y eventos.

PBM (Policy Based Management)

Este tipo de gestión modifica el rol del operador, no controla el sistema directamente, solo pasa a realizar funciones de la descripción de políticas, solventa problemas de gestión en los dispositivos complejos, como tal la gestión autonómica se encarga de estas configuraciones de auto-configuración, auto-reparación, auto-optimización y auto-protección, permitiendo automatizar el trabajo.

Redes alámbricas e inalámbricas

Las redes cableadas serán muy utilizadas por las aplicaciones SCADA las redes basadas en IP, M2M, son muy utilizadas por la cantidad de protocolos que manejan tales como SS7 (conmutación de paquetes que mantiene unido la conmutación de circuitos) y DOCSIS (estándar que permite la transferencia de datos a alta velocidad a un sistema de televisión) estas redes son opciones para plan de convergencia, actualmente DOCSIS proporciona internet por medio de HFC (hybridfiber-coaxial).

Las redes inalámbricas se clasifican de corto y largo alcance. En el grupo de corto alcance se encuentra NFC, PAN, LAN, MAN, RFID, WIFI, WiMAX etc. Dentro del grupo de largo alcance se encuentra WAN, GSM, CDMA, WCDMA o comunicación vía satélite. Se espera que aparezcan nuevos estándares en las redes inalámbricas para alcanzar lo propuesto en IoT.

Un ejemplo de cómo funciona un PLCs es que " la cadena de control es el bus que une los PLCs de los componentes de los dispositivos IoT que realmente hacen el trabajo, tales como sensores, actuadores, motores eléctricos, la consola luces, interruptores, válvulas, y contactores. El protocolo industrial común (CIP) es la base para una familia de tecnologías afines y tiene numerosos beneficios tanto para los fabricantes de dispositivos y los usuarios de los sistemas de automatización industrial. La primera de las tecnologías basadas en CIP, DeviceNet, surgió en 1994 y es una implementación del CIP sobre CAN (Controller Area Network), que proporciona la capa de enlace de datos para DeviceNet." (Fernando, 2014)pp 23-24.

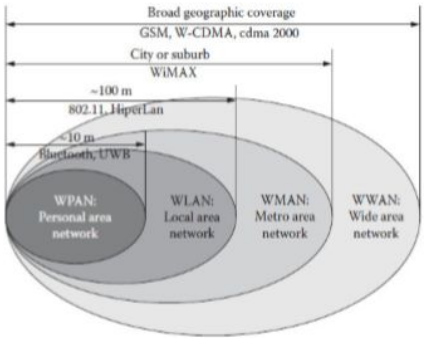

Figura 2. Clasificación Redes inalámbricas de corto y largo alcance.

Vulnerabilidades y soluciones en la integridad de seguridad de la información en el IOT

La ITU (unión internacional de telecomunicaciones), bajo la CCITT (comité consultivo internacional de telégrafos y teléfonos) en recomendación renombrada x.800 (arquitecturas de seguridad y aplicaciones en sistemas abiertos de interconexión.)

No entramos en enfoque a todo el documento, sino en si a ítems importantes dentro de la privacidad y seguridad en las de redes de datos, antes de entrar en detalles la recomendación x.200 genera unas definiciones a tener en cuenta, donde se nombran algunas:

Control de acceso: Difiere de una selección al medio o servicio de manera seleccionada por finalidad, previniendo el ingreso no autorizado.

Listas de control de acceso: numeración o listado de personal, entidades que poseen acceso autorizado a un recurso.

Responsabilidad: Garantizar el rastreo de acciones de una entidad, disponibles para la misma.

Amenaza activa: Amenaza que genera un cambio preconcebido en el sistema.

Autenticación: autenticidad de entidad par, origen de datos.

Integridad de los datos: promueve que los datos no se han alterados o destruidos mediante una amenaza.

Política: Imponencia de reglas o parámetro que se deben tener en cuenta al momento del uso de recursos y hacia quien va dirigido en búsquedas de generar seguridad frente a las amenazas.

Dentro del documento, la integridad de los datos es la propiedad de que estos mismos no sean alterados o arruinados de una manera no autorizada.

Firma digital, considerada aquella que podemos revisar para validar origen y privacidad de los datos.

Algunas de las aplicaciones de integridad de los datos mediante el uso de servicios de autenticación que promueven la reducción de amenazas tal como se indica en el siguiente proceso:

En cierta conexión se genera el uso de un servicio de autenticidad de la entidad par el preámbulo de la conexión de tal modo que este servicio aplicado como índole de la integridad nos permitirá obtener un historial de detección, duplicidad en los datos mediante usos de secuencias numéricas en el transcurso de vida de una conexión.

La integridad de los datos con recuperación indica que el servicio de subdivide para la integridad de todos los datos del usuario (x) en una conexión (x), detectando modificaciones, inserciones, eliminación de datos dentro de una secuencia del SDU(servicio de unidad de datos),con el intento de una restauración.

data communication networks: open systems interconnection (osi); security,structure and applications (recommendation x.800) 3.3.7, 3.3.19, 3.3.21, 3.3.26, 5.2.4, 5.2.4.1.

La IoT, como se ha implementado y el éxito que logra día a día, además por la cantidad de dispositivos que ya han sido conectados a internet y donde se pueden encontrar vulnerabilidades, ya que es un objetivo clave del ciberdelito. Por esta razón si hay un mal diseño en el objeto con interconectividad independientemente su medio, el usuario puede verse afectado por desprotegimiento de la información.En la actualidad las personas se han vuelto dependientes del funcionamiento de IoT por los servicios que ofrece pero no han llegado a analizar que las redes son inseguras.

IoT presenta ciertos problemas puesto que sus capacidades tiende a ser limitadas, generando inseguridad en las conexiones y difusión de información,permitiendo asi tipos de ataques de Denegación de servicio.

puesto al inconveniente con el ataque nombrado anteriormente se encuentran algunas posibles soluciones:

- Revisar los recursos de la red para la inversión en la seguridad por la vulnerabilidad de la información.
- Detección o monitoreo de anomalías, analisis de los datos transmitidos para la prevención de los ataques y evitar la propagación de este.
- Controlar tráfico generado por los dispositivos IOT por medio del Proxy.

IoT busca lograr dar mayor seguridad,mediante el uso de metodos en todos los contextos aplicados bajo su objetivo,generando asi una mayor resistencia,algunas de estas se pueden ver en un buen sistema de autenticación, sistema de control, monitoreo del envió de la información, puesto que hoy en día se han generado cambios en los tipos de comunicación peer to machine m2m, mejorando los procesos y ofreciendo diferentes servicios.

Existe 3 elementos fundamentales a tener en cuenta frente a la seguridad de la información: confidencialidad, integridad y disponibilidad, donde en nuestro relato nos enfocaremos a la privacidad en la cual se ven aspectos de violaciones de datos hechas por cracking, negligencia del empleado, datos en tránsito, robo de información

privilegiada, exposición accidental etc. Para que esto pase es por medio de la falta de políticas o procedimientos, la mala gestión del control de accesos o mala administración de la información sin tener un plan de continuidad que ayude a prevenir las situaciones de contingencia.

Se pueden encontrar diferentes estadísticas de vulnerabilidades de la información en diferentes países, los riesgos asociados que afecta la evolución de IoT y los inconvenientes en la integridad en la información.

Actualmente las empresas sienten preocupación por la fuga de información y la falta de disponibilidad, los riesgos más comunes son:

- Robo de información
- Ubicación mediante Dispositivos GPS
- Mal uso de los elementos IOT

Para analizar las vulnerabilidades de ataque al IoT se debe tomar en cuenta los vectores de ataque, los dispositivos IoT acceden por otros medios a una interfaz de administración, pues estos no tienen una entrada o salida de datos directa. Los usuarios no tienen los suficientes conocimientos de seguridad en los dispositivos, según el análisis que realizo Henry Castillo, que indica que el 86% de estos equipos tienen una configuración insegura.

Retomaremos de manera abreviada y general el comportamiento de las capas de arquitectura técnica compuesta del IOT

- Capa de percepción
- Capa de red
- capa de aplicación

La capa de percepción es la que identifica los tipos de objetos y recolecciona los datos,mediante dispositivos como sensores,teléfonos inteligentes,etiquetas de identificadores por radiofrecuencia(RFID) entre otros, donde luego son transferidos a la capa de red equivalente a un medio inalámbrico o alámbrico para que ocurra una propagación y transmisión de datos,mientras que la capa de aplicación es la de la interactividad con el usuario mediante interfaces y diferentes utilidades.

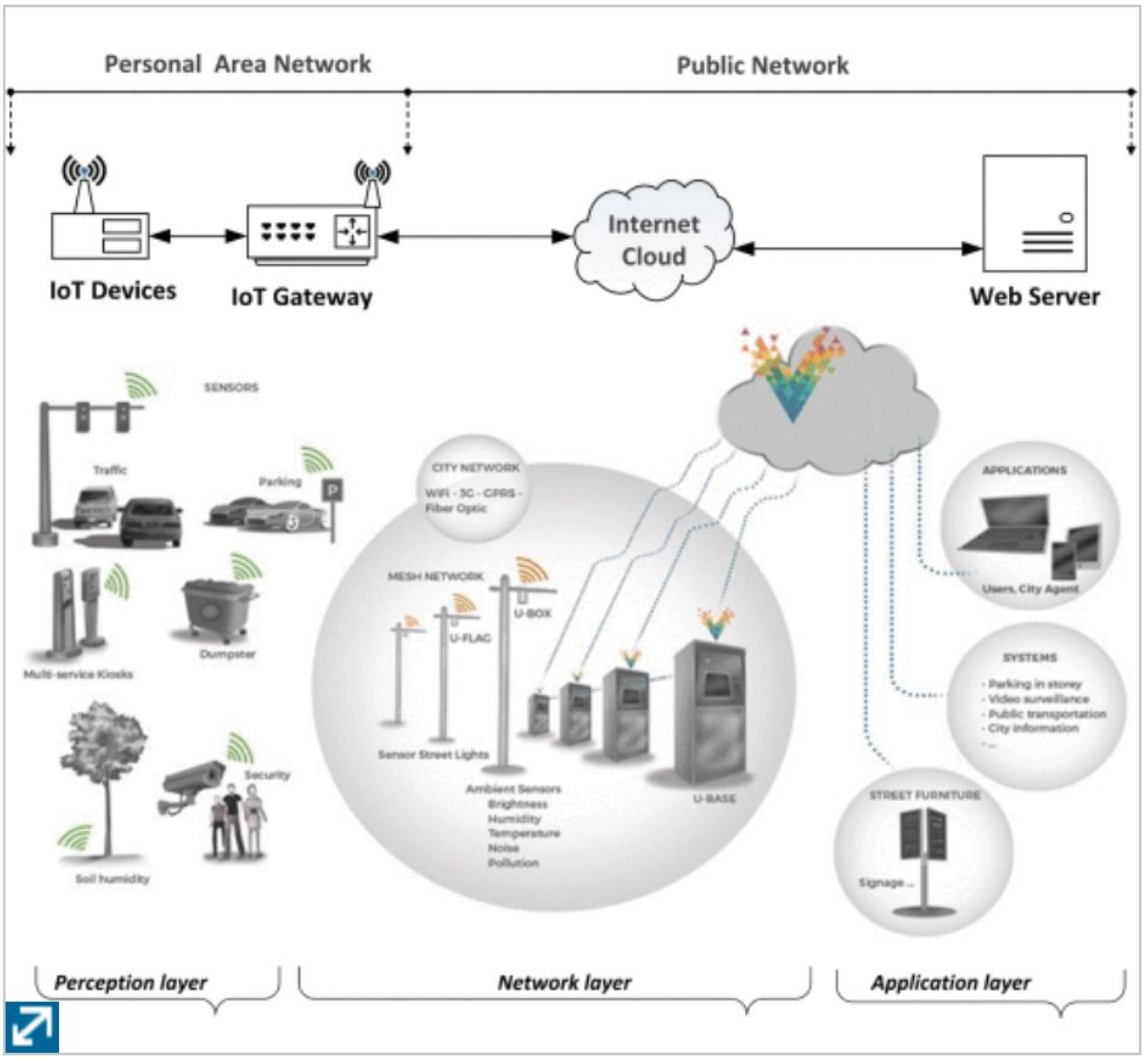

figura 3. Arquitectura genérica de capas del IOT y su aplicación.

Problemas de privacidad del IOT

La privacidad se define como el derecho de selección de qué la información personal de cada individuo de manera seleccionada es pública o no frente a las demas personas,donde de cierto modo esta se ve vulnerada bajo la división de tres espacios: la recolección de los datos,espacio de control del usuario y el espacio de conocimiento del usuario.

Identificación y seguimiento individual,perfil de usuario,interacción y presentación,transiciones del ciclo de vida,ataques de inventario y vinculación,donde el perfil de usuario es considerado la mayor amenaza .

Las U-city bajo conectividades ubicuas como se observa en la figura 4,presenta inconvenientes en relación con la privacidad acerca de la información personal e información de la vida diaria, tales como privacidad humana,privacidad de la ubicación y la privacidad del objeto.

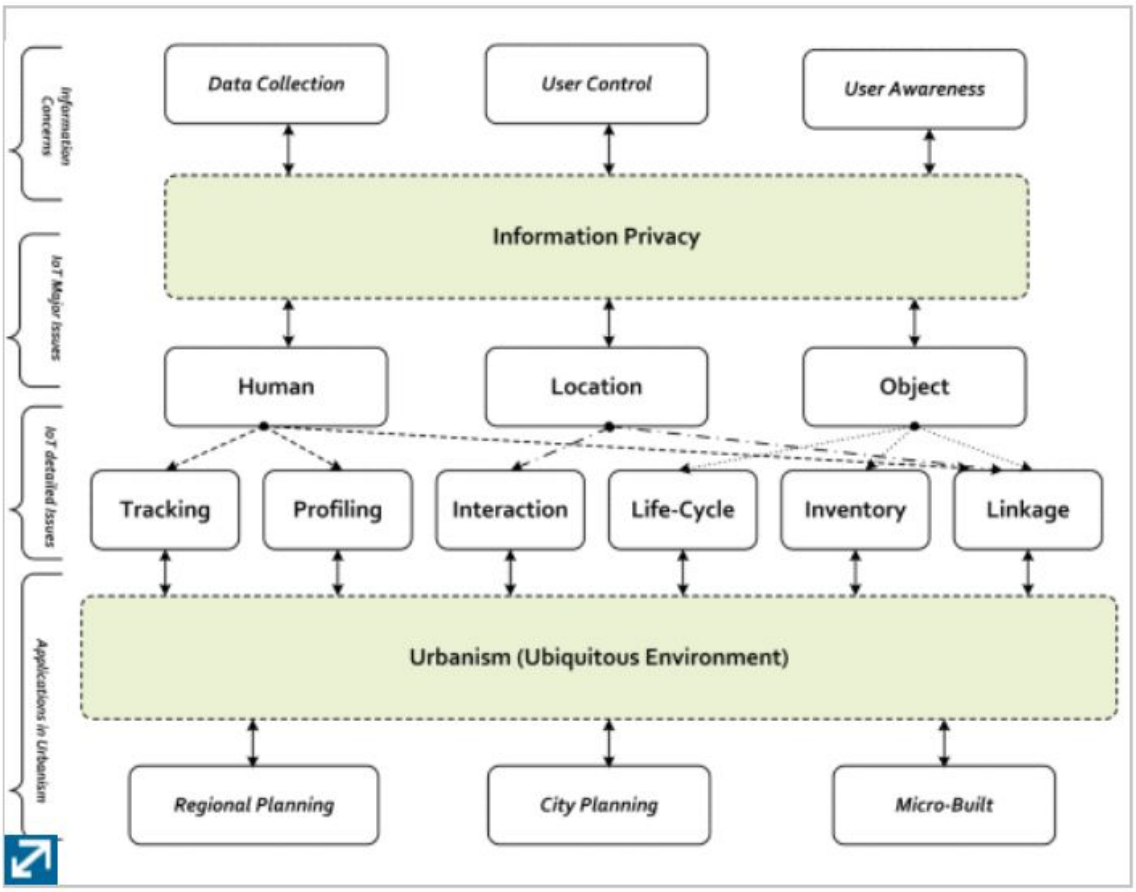

Figura 4. Entorno ubicuo y vinculación con el urbanismo desde varias perspectivas,y amenazas expuestas de la privacidad en los entornos.

Para garantizar la protección de los flujos de datos dentro de un ámbito IOT se recomienda poner atención a las puertas de enlace,entre otros requisitos como la mejora en la autenticación de datos,privacidad del cliente para generar inferencias sobre una persona en específica.

Se indica que el 25% de los ataques cibernéticos En el año del 2013 donde fueron alrededor de 750000 mensajes de correo electrónico tipo spam,provinieron principalmente de las cosas inteligentes, entre estos los electrodomésticos,donde el problema se establece desde la recopilación de datos por cada uno de los dispositivos por hogar y luego las ciudades inteligentes.

En busca de soluciones de privacidad de IOT a nivel urbano se da la opción de mejoras e implementaciones en la legislación de cada nación respecto a su manejo donde al igual se espera también leyes e iniciativa de la asociación internacional de privacidad sugeridas por la naciones unidas en búsqueda de dictámenes de protocolos de seguridad del IOT,donde así de cierto modo la capacidad de implantar sanciones fuesen igual en todos los países y los fallos fuesen los mismo tanto en el extranjero como en la nación,cuyos regímenes a actuar son las participaciones organizativas,gubernamentales y entorno legislativo donde los temas a tratar son privacidad,anonimato de datos,administraciones de identidad y de cómo estos se almacenan,recopilan,movimientos y manipulación de datos,ya que los datos IOT se encontraran rondando a un nivel global.

Al igual que en un ámbito empresarial multinacional IOT tendría dificultades frente a ancho de banda acceso y bloqueo de la nube de aplicación,donde para ello,en obtener una mejor calidad y control de flujo se vincula el big data.

hoy en día ha avanzado el uso de internet para el funcionamiento de los servicios y aplicaciones, principalmente comenzó la computación pero ha mejorado a que sea en la nube, allí se encontrara desde que empezó y como ha sido la evolución que ha tenido.

Actualmente ha sido muy fácil la implementación de la computación en la nube por bajos costos y porque la información se encuentra disponible desde cualquier lugar u hora, el internet de hoy ofrece video, datos y voz, pero con la implementación de internet de las cosas se puede comunicar cualquier objeto y hace referencia a que los objetos se convierten en nodos de comunicación a través de internet y que la comunicación entre el hombre y las cosas ya es un hecho.

La integración de computación en la nube e internet de las cosas busca optimizar ciertas cosas como; implementación de Ipv6, soporte de protocolos, eficiencia energética, seguridad y privacidad de los datos, calidad de servicio y almacenamiento de los datos.

Crece la ciberdelincuencia en las redes con diseños de malware actuales e innovadores de manera progresiva utilizando ataques de tipo mutación, donde en búsqueda de soluciones técnicas en defensa para este y demas atques se propone el uso de IDS e IPS.

(Alsunbul et al) nos muestra un sistema de defensa de red para detección de intentos de acceso no autorizado, mediante la presentación de un nuevo protocolo estándar, cuya finalidad es realizar una confusión en los intentos de sniffing; respecto al enrutamiento las rutas cambian periódicamente, para evitar accesos no autorizados y seguimiento de tráfico.

Zitta, Neruda y votech en el dispositivo frambuesa pi 3,aplicada para la alta frecuencia (uhf) e identificación por radio frecuencia(RFID),de lectores que utilicen protocolos (LLRP);fails2ban y suricata son los protocolos seleccionados por su alta escalabilidad,considerado el más adecuado para trabajo con sensores, nube y servidores

Suricata presenta mayor rendimiento frente a otro tipo de ids e ips como snort cuyas resultados fueron observados al lanzar un DDOS donde suricata respondió mejor a este en un solo núcleo al igual que en varios núcleos.

Chan y ramachandran proponen una seguridad multicapa para cloud computing,teniendo en cuenta que la criptografía es usada para proporcionar confidencialidad e integridad de los datos, de tal forma que en la primera capa de seguridad se plantea es la imposición de un firewall y controles de acceso, en la segunda capa se aplican

los ips e administración de identidad, en enfoque de eliminación de archivos maliciosos ,en la tercera capa se observa un cifrado convergente que genera una política de seguridad descendente, para el cual se realizaron pruebas de penetración cuyos resultados pronosticaron que el tiempo en que tarda en recuperarse de un acceso no autorizado está en un mínimo de 125 horas; otra de las soluciones de seguridad por Makkaoui, indica un modelo de seguridad y privacidad en la nube(CSPM) de varias capas, las cuales son:

(PESL) Capa de seguridad de infraestructura en la nube

(NSL)Capa de seguridad de red

(DL) capa de datos

(ACPML) control de acceso y capa de gestión de privilegios

Podemos observar que otra técnica mediante la mejora de autenticación de las VPN y uso de sistemas de posicionamiento global (GPS),proporciona protección de geo privacidad para móviles

Los honeypot y honeynet no pueden faltar, en este caso Olagunju y Samu implementaron un honeypot automatizado aplicando el uso de la técnica de gestión de sistema de registro centralizado (títere, máquinas virtuales),logrando recopilar información de dirección origen,hora,país de donde proviene el ataque, donde para ello lo primero a realizar es servir la presa hacia el atacante, un protocolo de transferencia de archivos es el indicado, ya que mediante estos los atacantes dejan ver sus rastros nombrados anteriormente.

Soluciones Técnicas de Clasificación por estructura de red.

En los métodos de clasificación de estructura de red, Filipe y hudec proponen un modelo de seguridad para redes MANET, cuyas redes orientadas en protocolos que permitan, eficiencia en ancho de banda respecto a las propiedades flexibilidad, movilidad.Los protocolos a utilizar son basados en RSA el cual es un protocolo seguro de enrutamiento incluyendo PKI ,firewall e IPS cuyos paquetes de enrutamiento están firmados y las claves son de carácter simétricas para cifrar el tráfico, mientras el IPS monitorea el tráfico alertando de nodos sospechosos, la consecuencia de llevar este planteamiento son encontrados con límites de tráfico debido a los dispositivos firewall,latenciade alta respuesta debido al envío de paquetes por cada nodo, comparación con base a búsquedas en bases de datos, cifrado y control.

Un IDS especializado para sensores de redes inalámbricas, con la utilización técnica de comparación de patrones, donde estos si coinciden, son administrados mediante el conjunto de políticas, reglas implantadas en el IDS, este después prosigue con un análisis de datos de recopilación, para luego ser comparados con políticas puestas en IDS,de obtener resultados frustrados este notifica una alerta.

Clasificación por aplicación

Los sistemas de riesgo electrónico de salud, se plantean en tres medidas preventivas aplicadas a la detección,prevención y corrección,empezando por el sistema de prevención,que mediante el uso de contraseñas y paráfrasis y varias maneras de autenticación ,todo esto obtenido bajo IDS/IPS para detecciones de un ataque,al igual que el manejo del control (administración,respaldos del sistema), que en caso de algún tipo de ataque,sea posible restaurar la configuración e administración.

Otra solución que se plantea es el desarrollo de un sistema inmune es la selección clonal conformada de un IDPS basado en host de manera híbrida obteniendo cantidad de datos para analizar.

Seguridad predictiva

Relativamente este tema o refrán ha salido hace poco,enfocado a la prevención en la seguridad cibernética, mediante la detección,reparación, y garantización de ataques existentes y a futuro dentro de las redes.

Noureddine et al. basado en la teoría general de la disuasión que está impulsado por la toma de decisiones del ser humano,realizaron estudios del comportamiento humano en la seguridad cibernética teniendo en cuenta campos como psicología, ciencias sociales, para lograr así la construcción de modelos predictivos de seguridad,donde

para indagar la efectividad de la seguridad de las contraseñas y auditorías, en frecuentes búsqueda de vulnerabilidades,teniendo en cuenta las herramientas que manejan el usuario en especial las de autenticación, se utilizó un estudio de caso para observar el comportamiento de los representantes de servicio al cliente y redes de actividad estocástica para la modelación de interacción de entre los empleados y las políticas de seguridad de la organización,cuyo modelado de estudio está dividido en varias fases,nombramos el primero desde la perspectiva del atacante,perspectiva de los empleados, y administradores, mediante técnicas de granularidad distinta por fase, cuya palabra se puede describir como la relación de cómputo a comunicación en un programa paralelo.

En cuestiones de protección de infraestructura Abraham y nahir propusieron la implementación de un nuevo modelo estocástico evaluando la seguridad enfocado a resultados de ataques frente a la infraestructura,donde luego se define un modelo markov (modelado estocástico para cambios de sistemas aleatorios) dependiente a variables en el tiempo teniendo en cuenta gráficas de ataques,teniendo en cuenta aspectos como la longevidad del ataque y tasa de descubrimiento de vulnerabilidad, para así mismo dar posibles resultados de ataques futuros de estados de seguridad de la red en actividad de detección de ataques día cero,mediante el marco de puntuacion de

vulnerabilidad CVSS, para la recolección de rasgos de explotabilidades complejas,como tipos de acceso,autenticación y vector de acceso,se llevaron otros estudios mediante los análisis de impacto, generación de gráficos para hacer uso del CVSS,dando resultados en cuanto a la explotabilidad,impacto y el alineamiento de inclusión de vulnerabilidades mediante el uso de un árbol de ataque.

En las antiguas secciones pudimos observar distintas soluciones de seguridad de enfoque en el IOT,sin embargo más allá de los estudios estocástico, aplicación de software IDS,IPS,IDPS.

Vemos que no se abarca toda la seguridad de los datos donde para ello al igual se propone la implementación del blockchain en conjunto de seguridad para el IOT,considerándolo una de varias ideas de seguridad de los datos puesto que el tráfico IOT va a ser expansivo y divulgado en varias redes de manera descentralizada,mediante el uso de blockchain y redes inteligentes que se hace de aplicación de la integridad de los datos.

Hablemos un poco de la tendencia desde el nacimiento de blockchain,utilizado originalmente para tipos de transferencias financieras de bitcoin,criptomonedas,donde cuyas transacciones son difíciles de rastrear y detectar fácilmente por un intruso.

El uso de blockchain para la seguridad IOT puesto que este tipo de lenguaje ha sido usado para registros,transacciones financieras, entre las cuales están las criptomonedas,el bitcoin,donde los resultados son transparencia y rastreo de detección de modificaciones,con base en esto se muestran dos formas de uso del blockchain a IOT

Primer tipo:

En esta forma podemos indicar que se crea el bloque cuando se ejecuta la transacción,este se propaga en todos los nodos de la red donde uno de estos nodos valida el bloque siendo este proceso llamado el minado en bitcoin,este luego lo esparce por la red,donde cada uno de los nodos agregan los respectivos bloques de acuerdo a su secuencia de su cadena de bloques.

Por otro lado el método dos consta de un intercambio de datos garantizando la integridad de los mismos haciendo uso de la métrica de integridad de referencia,de tal modo que este enfoque circula de la siguiente manera dentro de una red;se encuentra un punto centralizado cuyo propósito es mantener las referencias de repositorios miembros y de cierta manera se almacenan y se distribuyen los conjuntos de datos,cuyos datos como la información de dirección,membresía, propietario y uso compartido prevalece dentro de la cadena de bloques,independiente de la cadena de bloques del RIM (métrica de integridad de referencia)

se difiere del anterior método que cuando los conjuntos de datos son publicados disponibles,se encuentra la falencia cautelosa de un no manejo administrativo de tipo automatizado de anonimato en la publicidad de los conjuntos de datos antes de ser publicados,al igual otro tipo de reto a tener en cuenta frente a las implementaciones del blockchain

con IOT es el ciclo de vida del conjunto de datos respecto a su compartimiento con los demás nodos,puesto que los propietarios de un conjunto de datos no querrán la visibilidad constante de estos, después de realizar el registro de cadena de bloques,estos no pueden ser eliminados o modificados, de ser así se pierde la trazabilidad en la cadena,ya que allí se puede encontrar el RIM y los conjuntos de datos no se encontraran con la disponibilidad para su divulgación.

Podemos indicar algunas características del blockchain que de cierto modo puede garantizar las transacciones frente al IOT puesto que a su versatilidad y cadena de bloques en manejo descentralizado,mediante el respeto de la misma cadena de bloques,es decir tener un orden en cada uno de estos bloques identificados por una cabecera que es única y es conocida por su bloque siguiente de acuerdo a la secuencia(bloque 1, bloque 2) en cadena,donde maneja una llave pública que es transmitida a todos los nodos de la red y luego se utiliza criptografía asimétrica con cada uno de los mismos para las llaves privadas,otra característica que nos brinda blockchain en la integridad mediante la cadena de bloques es que las transacciones tienen que ser coherentes y basadas en una anterior transacción registradas en el sistema descentralizado de mineros y secuencia consecutiva sin saltos en los bloques por cada transacción,referente a las colisiones respecto a blockchain,debido a su uso descentralizado los mineros o nodos de este sistema trabajan de manera homogénea mediante la comunicación en la red de peer to peer, para la búsqueda de la solución y se notifica a los demás nodos que ya fue encontrada,podríamos indicar que el blockchain sería ese libro de bases de datos de todos las transacciones realizadas por p2p o m2m las cuales son registradas y divulgadas a todo los nodos de la red,de tal modo que nuestras transacciones son registradas en una red de máquinas a diferencia de los sistemas centralizados y donde no se genera un registro tan exacto de cada transacción o petición.

Detección de riesgos expuestos en el Firmware del IOT y de la proposición del blockchain como herramienta auto curable:

Podríamos enfrentar este tipo de inconvenientes cuando se nos presenta un ataque hacia un dispositivo expuesto IOT ya sea mediante la técnica de denegación de servicio distribuido,el cual es uno de los que más afecta este tipo de dispositivos,donde indicaremos que una de las posibles causas de que este dispositivo fuese expuesto, es por falta de parches de actualizaciones en el firmware,o por violación de técnica de ataque por fuerza bruta,donde en estos después de ser atacado el dispositivo,el personal de tecnología o infraestructura es el encargado de la solución al inconveniente donde de manera manual ejecutan el parche de actualizaciones donde de cierto modo no se garantiza la integridad,puesto que la solución está después de haber sucedido el hecho.

blockchain como base de datos distribuida encargada del seguimiento de cada una de las transacciones solicitadas y después registradas en cada uno de los dispositivos activos dentro de la red conservar todos estos la misma información

con transparencia, al menos que un ataque logre comprometer la principal parte de los nodos de la red,la integridad desde este aspecto no se logra comprometida, en el IOT con blockchain los firmware seran de autocuración y se auto actualizarán cambiando ciertos aspectos en firmwares normalmente usados que se guardan en un lugar seguro como el sistema raíz con un acceso de solo lectura.

La autocuración de los firmware de estos dispositivos por parte del blockchain es mediante la redundancia para sanar el software dañado,a través del reemplazo de código, o de cierto modo cuando se encuentra un firmware comprometido también es reemplazado por otro que de cierto modo tendrá las mejoras,actualizaciones,de todos estos procedimientos nombrados anteriormente, podemos obtener un acceso de registro de historia del firmware mediante la cadena de bloques.

Los dispositivos IOT deben contar con una interfaz de depuración,por ejemplo JTAG,ya que estos están siempre en red,para hacer posible de actualizaciones remotas,donde la autenticación es vital para no permitir modificaciones,donde luego de ser autenticado,una lógica de recuperación adapta el firmware nuevo,a través de la interfaz de depuración o red, que actualiza la memoria flash y calcula el RIM metadata.

Empecemos con la contextualización de los niveles del IOT los cuales son campo residencial o urbano,red de superposición y almacenamiento en la nube,donde los aspecto fundamentales son la seguridad, la descentralización, anonimato.

Veremos un enfoque de optimización de blockchain enfocado a una casa residencial.

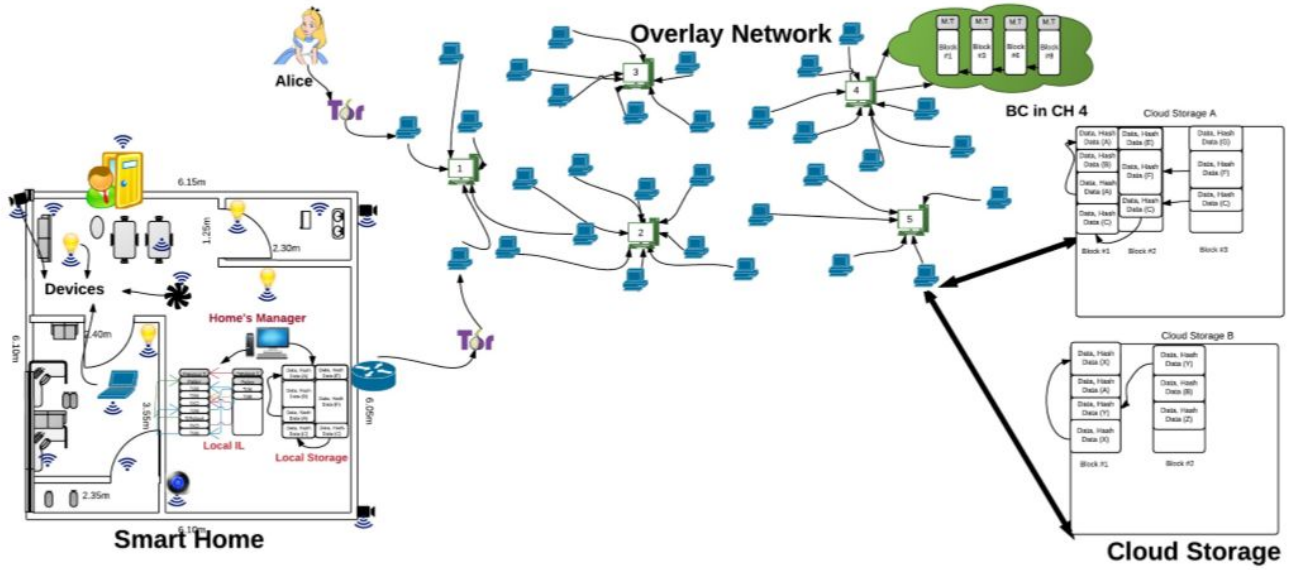

figura 5 Composición de una smart home mediante blockchain

La smart home dispone de un, IL local y un almacenamiento local como se observa en la anterior figura,donde los IL privado local asemejado a una administración blockchain pero de manera centralizada siendo dirigida por un SHM (administrador de casa inteligente),el cual procesa las transacciones entrantes y salientes mediante el uso de una clave compartida para la divulgación local,adicionalmente se administra un manejo de políticas prolongadas por el usuario para permitir o denegar difusiones en una red p2p,donde nodos como el SHM,teléfono inteligente o pc ayudarán en mejoras de latencia y sobrecarga en la red.

Para hablar acerca de una superposición en este ámbito,se refleja en formación de grupos,de tal manera que en cada uno de los grupos conformados seleccionan un líder de grupo (CH) bajo métodos. estos tienen un PK único,distinguido por otros CHs en la Superposición, la cual es aplicada para originar nuevos bloques para que otros CH den permiso de generar bloques,donde Cada nodo es libre de cambiar su cluster en caso de retrasos exagerados.

Los CH se componen para su funcionamiento de un directorio de pk de solicitantes y de PK con autorización de acceso a los datos de los SHM conectados a un cluster.

PK de solicitantes:Considerada la lista de PK que tienen permiso para acceder a datos

para los SHMs conectados a este cluster. Un ejemplo de lo que podría

Ser un SP que proporciona ciertos servicios para los dispositivos domésticos inteligentes.

PK de requisitos: La lista de PK de SHM conectados a este clúster, que están permitidos para ser accedidos.

Los CH superpuestos dentro del papel de blockchain público,que contienen un contenido mayor sobre cada uno de los nodos que se hospedan en la red superposición, el cual posee historial de transacciones realizadas por el usuario,en condiciones de solicitud y compartimiento de datos mediante la multisig, lo que indica es que cada transferencia es obligada a ser firmada por dos entidades donde se validan cada una de las transacciones del solicitante.

Para validación del usuario y en búsqueda de infiltrados mediante el historial de transacciones indica si el usuario puede o no tener acceso a realizar la transacción con base en el certificado específico con comparación del hash del PK de entrada con el de salida,donde los CH verifican los bloques generados de acuerdo a una secuencia y validación de bloque por los demás CH.

Al momento de la generación de un nuevo bloque,donde en parte también se produce una transacción multisig empleada para la generación de confianza,que luego es divulgada la misma transacción multisig,junto con los bloques a los demás CH vecinos,los cuales verifican las transacciones.

Hablemos ahora acerca de las transacciones de monitoreo las cuales son hechas en la red de superposición por los nodos hospedados allí recolectando datos en tiempo real tales datos del dispositivo y supervisión al procesamiento de transacciones .

VII. Bases legales de la investigación

La aplicación de las bases legales en IoT no es muy amplia en Colombia a pesar de que actualmente está siendo muy utilizada este tipo de tecnología en el área de la salud, ambientes inteligentes, sensores, transporte, consumo personal, redes sociales, industrias manufactureras por lo tanto la legislación establece deberes y obligaciones para asegurar el crecimiento continuo por medio de la calidad de los servicios y generando confianza en el consumidor.

Se podrá encontrar las políticas que debe tener en el área de las telecomunicaciones para que se pueda gestionar y licenciar en el espectro, asegurando la disponibilidad de una amplia gama de aplicaciones de IoT en bandas con o sin licencia. En el área de la privacidad debe establecer la obligación de la protección de los datos personales del consumidor brindando seguridad, transparencia, dando claridad y certeza del funcionamiento de los servicios de IoT contando con una infraestructura robusta, de alta disponibilidad y confiablidad.

De acuerdo al análisis de vulnerabilidades de seguridad de la información del IoT en busca de proteger la privacidad , se tendrá en cuenta las bases legales que esta necesita para cumplirse, respetar los derechos al usuario, compromisos del proveedor y protección de datos.

LEY 1273 de 2009[2]

A través de esta ley se enfoca a la protección de la información y de los datos, cada artículo especifica desde el acceso abusivo a un sistema informático, interceptación de datos informáticos, daños o uso de software malicioso etc. como tal esta ley se encarga de asegurar la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y aplica en el análisis de vulnerabilidades del sistema.

LEY 1341 DEL 30 DE JULIO DE 2009[3]

Esta ley define los principios y conceptos sobre la sociedad de la información u organización de las tecnologías de la información y las comunicaciones, se encarga de ordenar, controlar que los recursos sean eficientes, dirigidos por el sector de las tecnologías, como tal busca dar uso eficiente de la infraestructura dar prioridades al uso de las tecnologías de la información y proteger los derechos del usuario.

CONPES 3701[4]

Lineamientos de política para ciberseguridad y ciberdefensa para las amenazas informáticas desarrollando la prevención y control en la seguridad de la información como tal es un compromiso del gobierno nacional, por la evolución que está presentando las nuevas tecnologías, este lineamiento incluye las anteriores leyes expuestas para ejercer la estrategia de ciberseguridad.

Ley 1581 de 2012 proteccion de datos personales.

Esta ley aplica la seguridad, confidencialidad y transparencia de la privacidad del usuario, regula el derecho al Habeas Data y derecho a la información, es definida por el alcance, principios, derechos de acceder a los datos personales y aplica para el respaldo de la información que guarde el usuario cuando implemente el manejo de los dispositivos IoT.

[2]Ley 1273 de 2009 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos 5 de enero de 2009 p-1.

[3] Ley 1341 de 2009 marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones 30 de julio 2009 p-34.

[4]Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación Bogotá D.C., 14 de julio de 2011p.1- 43.

Norma ITU [5]

Unión Internacional de Telecomunicaciones – ITU es encargado de regular las telecomunicaciones se enfoca en 3 sectores como: radiocomunicaciones, normalización y desarrollo, son importantes para el funcionamiento de las redes, acceso a internet, protocolos etc. realizan conferencias y se encargan de dar las recomendaciones en distintas empresas.

Impacto de la privatización y regulación de las telecomunicaciones en estructuración de la industria

Norma Iso 27001 [6]

ISO 27001 gestión de la seguridad de la información considera que la información debe estar protegida, se enfoca a preservar la integridad, confidencialidad y disponibilidad de la información, define el alcance, analiza los riesgos y los gestiona, se implementa control de riesgos medidas preventivas y correctivas para identificar las vulnerabilidades, amenazas y por ultimo tratar el riesgo.

Norma Iso 27002 [7]

Dominio de política de seguridad es un estándar que complementa ISO 27001 se enfoca a todo tipo de empresas aplicando buenas prácticas para la gestión de la información y controles establecidos en la norma 27002, esta norma incluye la política de seguridad de la información, organización, seguridad física y del medio ambiente, control de acceso, adquisición desarrollo y mantenimiento de sistemas, gestión de incidentes de seguridad de la información y gestión de continuidad para asegurar que las operaciones sean recuperadas para evitar la violación informática.

[5] Norma ITU Unión Internacional de Telecomunicaciones 1865 estas recomendaciones son fundamentales para las redes TIC.

[6] Norma ISO 27001 año 2013, sistema de gestión de la seguridad de la información para evaluar el riesgo y aplicar controles para tratarlos o eliminarlos.

[7] Norma ISO 27002:2013 mejora las prácticas en la seguridad de la información establece principios para mejorar la gestión de la seguridad de la información.

CAPITULO III

DISEÑO METODOLÓGICO

En este artículo se podrá encontrar los diferentes significados que tiene IoT, desde que se conoció este término fue referenciado con varias definiciones tanto para la Comisión de la Unión Europea, como para la Unión Internacional de Telecomunicaciones (ITU)

IOT busca ayudar en muchos aspectos y todos los campos que se pueden abarcar bajo una producción,donde lo ideal es que con base a lo que se cree el dispositivo tendrá un objetivo y finalidad donde se recopila información y llega a un destino,al igual que en busca de mayor exactitud y producción.

Con base a lo anterior IOT vislumbrara por su apoyo en todos los aspectos, pero nos damos de cuenta que con base al relato anterior es escéptico, su evolución y creación donde los seres humanos si no son capacitados de los riesgos que puede tener una implementación de IOT,seremos consumidores de hipnotismo y atracción en búsqueda de una evolución que se inundara en datos de tráfico por todas la redes sin importancia alguna de que nuestros datos y privacidad sea expuesta,ya que al haber tanto dispositivos conectados da más opciones a un atacante para poder ingresar a este sistema,violando derechos humanos de manera cibernética y de los consecuentes que hay respecto al consumo de elementos electrónicos no amigables para el medio ambiente y ciclos de vida muy cortos,por ende no se querra decir que IOT será la decepción pero se requiere más atención a temas de la accesibilidad,autenticación,seguridad en estos elementos y por ende informar a la gente de que la tecnología IOT tiene sus riesgos,donde ya para lo cual el ciudadano no será compulsivo al momento de la demanda de productos IOT y pensara mejor al momento de la compra de un producto IOT.

Podemos indicar que podemos encontrar soluciones mediante el uso de varios medios tales que por software,infraestructura,hardware,lenguajes de programación,entre otros,donde para lo cual el único objetivo, protección de la información de datos del IOT y que este no sea un tipo de vulnerabilidades para cualquier tipo de redes y acceso.

Todos los medios son válidos desde que se garantice la integridad de la información y no genere un riesgo la incorporación del IOT a nuestras redes existentes.

En la IOT podemos validar que se genera una interconexión de dispositivos semiconductores conectados en la red de manera exponencial en comunicaciones persona-maquina, maquina-maquina,al igual que las redes de datos y su clasificación de ciudades inteligentes,redes autónomas,inteligentes al igual que las últimas implementaciones de sistemas de salud inteligentes.

Desde que llegó IOT al mundo real uno de sus prevalecientes ha sido la seguridad,hay facilidades de conectividad y comunicación, pero no se garantiza un cubrimiento total e integridad de datos de tráfico de esos dispositivos interconectados con ciertas finalidades.

Esta solución es muy interesante y grandiosa puesto que hay integridad frente a los datos,entre otras como el uso del blockchain.

Observamos que la tecnología del futuro tendrá que estar relacionada con el blockchain por su robustez y manejo de transacciones mediante la cadena de bloques garantizando la integridad de conjuntos de datos respecto a que hay un manejo público,y divulgación de esta de manera descentralizada.

El incremento de energia sera alguna de las consecuencias que presentan el blockchain debido a su manejo de transacciones por red mediante mineros,hash,cabeceras,transacciones,donde para lo cual se tiene que buscar otros métodos de alimentación del sistema ya que si lo planteamos desde un nivel empresarial los incrementos de energía en algunos casos sobrepasan lo permitido

IOT con blockchain garantizarían más la integridad de los datos puesto que al momento de ser pública la información a los nodos mediante la cadena de bloques la cual lleva el consecutivo de transacciones que no permite alguna alteración o si se presenta se puede detectar donde está la intrusión al orden consecutivo de bloques y registros de transacciones anteriores y el manejo de broadcast para su comunicación,donde los nodos disponibles de la red reciben la misma información.

De Acuerdo a la información ya estipulada, la implementación de Blockchain con IoT sería una combinación perfecta para dar tranquilidad al usuario, ya que no cuenta con el conocimiento técnico para conocer de fondo las vulnerabilidades del sistema, sería la mezcla entre ofrecer seguridad con un ancho de banda 5G y flexibilidad de IoT para cubrir todas las necesidades en todos los ámbitos.

Es factible la idea de optimización de blockchain aplicado a la seguridad del IOT donde el ejemplo propuesto en el documento se refiere a una smart home, puesto que blockchain requiere de alta escalabilidad,altos recursos de energía y procesamiento donde en combinación de una arquitectura centralizada bajo los IL como libro de datos de

toda la red de superposición genera menos consumo de recursos frente al funcionamiento de un bitcoin,donde de cierto modo se garantiza la privacidad y anonimato,donde al momento de un intruso quiera modificar bloques o realizar peticiones de transacciones es poco factible de sea exitosa puesto que si no están desde un registro primario en el IL,descarta tanto las transacciones como los bloques, y al igual la implantación de políticas de transacciones del usuario,de tal modo que un ataque DOS que es de los más ejecutados en los elementos IOT cuenta con una poca probabilidad de ser satisfactorios.

Se busca que la comunicación sea de dispositivo a usuario y de dispositivo a dispositivo para aprovechar al máximo estos enlaces de la comunicación móvil 5G, poder incrementar la vida útil de los dispositivos menos robustos y mantener la estrategia de recolección de energía para que aumente el tiempo de vida del sistema.

VIII. Tipo de investigación

Conjunto de características de una investigación con respecto a su naturaleza y metodología y la técnica a emplear en el proceso de búsqueda de la solución del problema planteado.

Toda investigación sin excepción debe:

Identificar:

- Propósito: Investigación básica o aplicada
- Lugar: Investigación documental, experimental o de campo
- Alcance: Investigación descriptiva, argumentativa o correlacional

Definir:

o Cada uno de los tipos de investigación identificados anteriormente, conforme a los desarrollos del autor o teórico que el investigador tenga a bien considerar.

Argumentar:

o Por qué se identificó el tipo de investigación y de qué manera se relacionó con la propuesta presentada.

IX. Población

- Aquí se describen las características generales y/o particulares de las unidades de análisis.

- Se deben incluir los criterios de elección (inclusivos y exclusivos) para la integración de las muestras o delimitación de los informantes, si es el caso
- Desarrolla las características de las personas a las que van orientadas las intervenciones o el brief de las piezas comunicativas en ejecución.

X. Técnicas e instrumentos de recolección de datos

- Definir los instrumentos con los que se compiló o recolectó la información o datos para resolver la pregunta de investigación formulada anteriormente. (encuestas, entrevistas, grupos focales, etc).
- Se debe presentar la versión del instrumento final de investigación
- Se anexa el instrumento a implementar sin diligenciar
- Se presentan los bloques de información solicitadas
- Se justifica la utilidad de las preguntas realizadas y los hallazgos encontrados

CAPITULO III

RESULTADOS DE LA INVESTIGACIÓN

XI. Resultados del objetivo específico no. 1

Indicar el proceso que se llevó a cabo para obtener el logro del objetivo No. 1; a partir de la constatación de datos, informantes, o revisiones bibliográficas indicadas en el marco metodológico.

Es importante que la argumentación presentada incluya los soportes o pruebas del proceso realizado (gráficos de barras, circulares, frecuencias, etc); así como la presentación final de los tangibles del diseño que se propusieron en el objetivo en desarrollo (caracterizaciones, bocetos, documentos grises –borradores- del proceso)

XII. Resultados del objetivo específico no. 2

Indicar el proceso que se llevó a cabo para obtener el logro del objetivo No. 2; a partir de la constatación de datos, informantes, o revisiones bibliográficas indicadas en el marco metodológico.

Es importante que la argumentación presentada incluya los soportes o pruebas del proceso realizado (gráficos de barras, circulares, frecuencias, etc); así como la presentación final de los tangibles del diseño que se propusieron en el objetivo en desarrollo (caracterizaciones, bocetos, documentos grises –borradores- del proceso)

XIII. Resultados del objetivo específico no. 3

Indicar el proceso que se llevó a cabo para obtener el logro del objetivo No. 3; a partir de la constatación de datos, informantes, o revisiones bibliográficas indicadas en el marco metodológico.

Es importante que la argumentación presentada incluya los soportes o pruebas del proceso realizado (gráficos de barras, circulares, frecuencias, etc); así como la presentación final de los tangibles del diseño que se propusieron en el objetivo en desarrollo (caracterizaciones, bocetos, documentos grises –borradores- del proceso.

CAPÍTULO V.

CONCLUSIONES Y RECOMENDACIONES

Se indica el proceso que se llevó a cabo para obtener el logro del objetivo general; a partir de la constatación de datos, informantes, o revisiones bibliográficas indicadas en el marco metodológico.

Es importante que la argumentación presentada incluya los soportes o pruebas del proceso realizado (gráficos de barras, circulares, frecuencias, etc); así como la presentación final de los tangibles del diseño que se propusieron en el objetivo en desarrollo (caracterizaciones, bocetos, documentos grises –borradores- del proceso)

No se deben repetir acciones que se realizaron previamente en los resultados de los objetivos específicos.

Se realizan apreciaciones sobre la importancia que tuvo la realización del trabajo, así como sugerencias para que otros compañeros puedan mejorar en sus procesos de investigación

BIBLIOGRAFÍA

Realice un inventario de las fuentes bibliográficas o digitales consultadas de acuerdo con las normas IEEE (Institute of Electrical and Electronics Engineers)

XIV. Adecuación de estilo

Tipo de letra: Times New Roman o para el caso de los documentos institucionales de la Fundación Universitaria San Mateo: **Century Gothic**. Otros tipos de fuentes que puede ser empleada en caso especial, será: **Courier** para referenciar direcciones electrónicas**.**

Tamaños y tipos de letra:

- Título del capítulo (titulo 1): 24 puntos, centrado,
- Subtitulo nivel 1 (titulo 2): Mayúscula, 10pts, centrado, numerado con números romanos.
- Subtitulo nivel 2 (titulo 3): 10 pts, cursiva, alineado a la izquierda, numerado con letras.
- Subtitulo nivel 3 (titulo 4): 10 pts, cursiva, alineado a la izquierda, numerado con números arábigos.
- Contenido del documento: 9pts.
- Referencias de objetos: 8pts.
- Títulos de figura: 8pts.
- Información de tablas: 8pts.
- Posición: Justificado.

Figuras y tablas

El tamaño para los títulos de las tablas, figuras y notas al pie de página es de 8 puntos. Todas las figuras y tablas deben aparecer centradas en la columna (las figuras y tablas de gran tamaño podrán extenderse sobre ambas columnas).

Evite ubicar las figuras y tablas en medio de las columnas, siendo preferible su ubicación en la parte superior de la página. Se aconseja que inserte la figura o la tabla, junto con su descripción, en un cuadro de texto, tal como se hace en este documento.

La descripción de las figuras deberá ubicarse debajo de las mismas, centrada, numerándose con cifras arábigas. Use la abreviatura Fig. n tanto para etiquetar la figura o gráfico como para referirse a ella.

La descripción de las tablas deberá ubicarse encima de las mismas, numerándose con cifras romanas y con el texto en versalitas. La etiqueta de la tabla (Tabla X) debe escribirse en mayúsculas y encontrarse sola en una línea. Use Tabla X para referirse a una tabla.

Los pies de las figuras y de las tablas deben seguir el formato mostrado bajo la Fig. 1 y bajo la tabla 1. Si es posible, utilice un formato vectorial (como EPS o PDF) para representar diagramas. Los formatos de tipo *raster* (como PNG o JPG) suelen generar ficheros muy grandes y pueden perder calidad al ampliarlos.

Ecuaciones

Las ecuaciones deben estar centradas y situadas en líneas distintas. Cada ecuación debe ser numerada:

$$E = mc^2 \qquad (1)$$

Para referenciar una ecuación, utilice Ec. 1.

Referencias

Las referencias serán numeradas en orden de aparición [1]. El formato de referencias será el estándar del IEEE. Se muestra algún ejemplo en el apartado correspondiente.

[1] J. Díaz-Verdejo, "Ejemplo de bibliografía", En Actas de las XI Jornadas de Ingeniería Telemática, vol. 1, n. 1, pp. 1-5, 2013.

[1] Salazar, J., & Silvestre, S. (2016). Internet de las cosas. Techpedia. České vysoké učení technické v Praze Fakulta elektrotechnická.

[2] Sosa, E., & Godoy, D. (2014). Internet del futuro. Desafíos y perspectivas. Revista de Ciencia y Tecnología, 16(21), 40-46.

[3] García, L., & Carlos, L. (2015). Estudio del impacto técnico y económico de la transición de internet al internet de las cosas (IoT) para el caso Colombiano (Doctoral dissertation, Universidad Nacional de Colombia).

[4] Alberto, J. P. L., Adrián, V. V. W., & Fernando, V. E. N. (2014). Estado del arte de las arquitecturas de internet de las cosas (iot).

[5] Soraya Pinagua (2012). Un poco de historia sobre Internet de las Cosas http://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/#comments