

**REFERENCIA AL CONSEJO**

1. Según el informe Deloitte hay aumento del tráfico de redes después de la pandemia y un crecimiento exponencial del espacio digital donde se brindan cada vez más servicios que requieren de una seguridad más eficiente y robusta como transacciones, servicios en la nube para infraestructura de negocios, o almacenamiento de información sensible que puede ser robada.
2. Adicionalmente, con el despliegue de las redes 5g hay un aumento de dispositivos de todo tipo conectados a internet lo que se denomina el Internet de las cosas cada año, se prevé según el portal de estadísticas Statista que en 2030 habrá más de 29.000 millones de dispositivos conectados en todo el mundo y tan solo 19.000 millones de dispositivos en 2025.
3. Los ataques cibernéticos en Colombia aumentan cada año, pero además la complejidad de estos ataques también aumenta. los ciber atacantes se mantienen a la vanguardia, creando técnicas de ataque cada vez más sofisticadas que utilizan incluso aprendizaje de máquinas e inteligencia artificial, por esto es posible que pronto, el gran volumen, la sofisticación y la dificultad de detectar ciberataques sobrepase la capacidad humana.
4. la IA es un multiplicador de fuerza, que permite que los equipos de seguridad no solo respondan más rápido de lo que pueden moverse los atacantes cibernéticos, sino que también anticipen sus movimientos y actúen con anticipación.

OPCION 2

El siguiente proyecto consiste es crear un modelo de aprendizaje profundo que pueda predecir ataques DDoS en redes IoT.

Una de las soluciones eficaces para prevenir las intrusiones ante su constante complicación y crecimiento cuantitativo son la monitorización y análisis de tráfico multifuncional.

El monitoreo del tráfico de red hoy en día está dirigido principalmente a la detección rápida de "ráfagas" de tráfico de red de la red de infocomunicación, que son el resultado de accesos no autorizados, virus, ataques, intrusiones y otras amenazas a la seguridad de la información.

Entre estas amenazas, los ataques DDoS (Distributed Denial of Service) son los más comunes estos son bastante difíciles de detectar debido a la gran cantidad de fuentes de ataque y las características del tráfico.

Una red de robots (botnet) hace referencia a un grupo de equipos que han sido infectados por malware y se encuentran bajo el control de un agente malicioso. El término botnet es una contracción de las palabras robot y "network" (red) y cada dispositivo infectado se denomina Bot. Las redes de robots (botnets) pueden diseñarse para llevar a cabo tareas ilegales o maliciosas, como enviar spam, robar datos, distribuir ransomware, hacer clic en anuncios de forma fraudulenta o realizar ataques de denegación de servicio distribuido (DDoS).

Los datasets disponibles son diferentes. Cada dataset tiene un conjunto de características diferente.

Los modelos de IA que se diseñan solo funcionan para un dataset especifico.

No se puede evaluar el desempeño de un modelo con otro dataset solamente con el dataset especifico para el que fue diseñado.

Para que estos modelos tengan una mayor utilidad y para que puedan implementarse en escenarios reales es necesario crear una estandarización de las características capturadas de los datasets para el entrenamiento.

Para estandarizar las características se utiliza el protocolo netflow que permite rediseñar los datasets existentes y crear un conjunto de características común que permita evaluar modelos con diferentes datasets.

Netflow permite una extracción fácil de características del flujo de red.

Debido a esto se podrán utilizar modelos en escenarios reales diversos y evaluar su desempeño reformulando su diseño con mayor facilidad.

**RESUMEN EJECUTIVO**

La implementación de las nuevas redes 5G traen consigo el desarrollo y crecimiento de lo que se ha llamado el Internet de las cosas.

El crecimiento y despliegue de redes de dispositivos IOT a nivel comercial e industrial requiere un gran esfuerzo para que estas cuenten con la debida seguridad.

Debido a que los atacantes se encuentran en una búsqueda constante de nuevos métodos para vulnerar los sistemas y entre estas amenazas, los ataques DDoS (Distributed Denial of Service) son los más comunes y son bastante difíciles debido a su variedad y las características del tráfico.[]

La IA incluyendo machine learning y más específicamente Deep learning ha probado ser una herramienta eficaz y altamente precisa para detectar y proteger las redes contra los ciberataques.[]

sin embargo debe avanzarse en una forma estandarizada de captura de características en los datasets de entrenamiento para que los modelos puedan ser evaluados utilizando diferentes datasets y puedan ser implementados en escenarios diversos de forma mas sencilla.

Por lo tanto en el presente trabajo se propone el diseño, la implementación y evaluación de un modelo de Deep learning que detecta y previene ataques DDoS utilizando un dataset basado en el protocolo de red netflow el cual toma ráfagas de red en forma de flujos,

y mediante estos se puede detectar los comportamientos de la red que están fuera de lo “normal” y que son el resultado de accesos no autorizados, virus, ataques, intrusiones y otras amenazas a la seguridad de la información.

**PLANTEAMIENTO DEL PROBLEMA ¿Cuál es la situación actual?**

Las redes IOT son cada vez más grandes por la gran cantidad de dispositivos de bajo coste que son capaces de conectarse a internet como cámaras, grabadoras de video, electrodomésticos y el sector industrial sobre todo sensores y con esto

aumenta la complejidad de los ataques a estas redes y también su volumen por lo que la dificultad de detectar ciberataques es cada vez mayor y sobrepasa la capacidad humana.

Los dispositivos IOT no están siendo diseñados para ser seguros y cuentan con una variedad de vulnerabilidades como contraseñas débiles o codificadas, falta de un proceso o mecanismos de actualización, servicios de red e interfaces de ecosistema no seguros, componentes de la aplicación IoT obsoletos o no seguros, almacenamiento y transferencia de datos no seguros a partir de estas vulnerabilidades se crean amenazas como suplantación de identidad, divulgación de información, manipulación de datos, elevación de privilegios. []

Entre los principales ataques que explotan están vulnerabilidades están los que se realizan mediante botnets, que se caracterizan porque permiten realizar ataques distribuidos de denegación de servicio (DDoS), que sobresaturan el tráfico de acceso con el fin de inhabilitar o tomar el control de los dispositivos. []

El problema de los ataques de DDoS se vuelve cada vez más difícil debido a la gran cantidad de dispositivos de IOT que se conectan a la red con poca o ninguna seguridad. [] Los ataques DDoS estuvieron entre los principales ciberataques entre el año 2013 y 2020 como lo indica una revisión hecha en 2021 sobre la seguridad en IOT. [] Y son bastante conocidos los ataques DDoS a servicios como amazon web services, github o también a empresas como CNN, Dell, E-Trade, eBay spamhaus o el proveedor de nombres de dominio DYN[]

La IA para crear IDS (sistemas de detección de intrusos por sus siglas en inglés) ha probado ser una herramienta eficaz y altamente precisa para detectar y proteger estas redes contra los ciberataques convirtiéndose en un multiplicador de fuerza para los grupos de ciberseguridad, sin embargo, su implementación en entornos reales tiene una serie de dificultades. []

La IA es posible gracias a la captura de una gran cantidad de datos. Los datos de red reales son difíciles de obtener debido a cuestiones de seguridad y privacidad por lo que se desarrollan bancos de prueba para obtenerlos y mediante estos se capturan los datos que conforman los datasets para el entrenamiento de los modelos de Inteligencia artificial. Pero esta captura no es estandarizada por lo que se crean datasets de entrenamiento con características muy diferentes.

Las características de los datasets determinan el desempeño de los modelos por lo que no se puede medir el desempeño de un modelo creado con un dataset en otro dataset ya que se crean modelos para dataset específicos y por lo tanto para entornos de prueba específicos por lo que no se pueden utilizar estos modelos en otros dataset y en otros entornos. Adicionalmente los entornos de prueba son diferentes a los entornos reales por lo que no se pueden aplicar los modelos desarrollados para estos entornos de prueba en la mayoría de entornos reales.

Por otra parte, en los dataset existentes se utilizan complejas técnicas de extracción, recopilación y almacenamiento que no son viables de utilizar en redes reales con un alto tráfico por lo que se necesitan utilizar formas más sencillas de capturar características de trafico de red para crear datasets a lo que se le pueda aplicar aprendizaje profundo.

El planteamiento del problema parece estar bien estructurado y aborda una problemática actual en el ámbito de la seguridad de redes IoT. Sin embargo, se pueden realizar algunas correcciones y sugerencias para mejorarlo:

Es recomendable incluir una introducción que permita al lector comprender el contexto y la importancia del problema que se va a abordar. Por ejemplo, se podría mencionar el aumento de la conectividad en la actualidad y cómo esto ha llevado al surgimiento de nuevos riesgos de seguridad en las redes IoT.

En el primer párrafo, se podría incluir una referencia o fuente que respalde la afirmación de que la dificultad de detectar ciberataques sobrepasa la capacidad humana.

En el segundo párrafo, se sugiere mencionar algunas de las posibles consecuencias de las vulnerabilidades de los dispositivos IoT, como por ejemplo la interrupción de servicios, el robo de información o la propagación de malware.

En el tercer párrafo, se podría explicar con más detalle cómo funcionan las botnets y qué consecuencias pueden tener para las redes IoT.

En el cuarto párrafo, se podría indicar cómo la IA puede ayudar a resolver los problemas de seguridad en las redes IoT de manera más eficiente que los métodos tradicionales de detección de intrusiones.

En el quinto párrafo, se podría mencionar que la falta de estandarización en la captura de datos también puede tener un impacto en la interoperabilidad entre diferentes sistemas de IA de detección de intrusiones.

En el último párrafo, se podría ofrecer algunas sugerencias para simplificar la captura de características de tráfico de red, como por ejemplo la utilización de técnicas de muestreo o la implementación de sistemas de recopilación de datos más eficientes.

En general, el planteamiento del problema parece estar bien fundamentado y se abordan aspectos importantes relacionados con la seguridad de las redes IoT.

**2.2 JUSTIFICACIÓN**

¿Por qué lo hago? ¿Cómo beneficia a la universidad? ¿Cómo aplico lo que vi en la carrera? (mínimo 3 párrafos de 6 líneas y máximo 1 pagina) ¿para que se va hacer

Se están desarrollando e implementando nuevos tipos de redes y las organizaciones empresariales y gubernamentales se están teniendo que enfrentar a las brechas de seguridad en estos nuevos sistemas tan solo en la primera mitad del año en Colombia se presentaron aproximadamente 6.3 millones de intentos de ciberataques, convirtiéndolo así en el tercer país más atacado de américa latina.

Además, no solo aumentó la cantidad de ataques con respecto a años anteriores, sino que las herramientas son más sofisticadas.[3]

La IA cibernética puede ser un multiplicador de fuerza, lo que permite que los equipos de seguridad no solo respondan más rápido de lo que pueden moverse los atacantes cibernéticos, sino que también anticipen estos movimientos.[1]

Para la realización de este proyecto se utilizarán los conocimientos de redes específicamente en cuanto a redes de paquetes e ingeniería de tráfico, se utilizarán las herramientas en desarrollo de software y programación adquiridas entre otras utilizando el lenguaje de programación Python, y se utilizarán las habilidades para el modelamiento matemático adquiridos durante la carrera, además de los conocimientos sobre seguridad informática en cuanto a tipos de ataques.