UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

MAYO 2023-SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

LA INTELIGENCIA ARTIFICIAL EN LA DETECCION DE INTRUSIONES EN ENTORNOS DE REDES DEFINIDAS POR SOFTWARE (SDN)

ESTUDIANTE:

JANETH LISSETTE ZAMBRANO MORAN

TUTOR:

ING: MEJÍA VITERI JOSÉ TEODORO

AÑO 2023

RESUMEN

Las Redes Definidas por Software (SDN) representan una innovación en la gestión de redes al proporcionar una flexibilidad y eficiencia significativas en su funcionamiento. Sin embargo, esta flexibilidad y eficiencia también conlleva importantes desafíos de seguridad. El aumento constante de las amenazas cibernéticas se ha convertido en una seria preocupación, especialmente debido a la arquitectura centralizada de SDN, que se basa en controladores lógicos para monitorear los flujos de datos en toda la red. La solución propuesta incluye la aplicación de inteligencia artificial (IA) en la mitigación de ataques, aprovechando la capacidad de analizar datos y detectar patrones anómalos en tiempo real, esto implica la identificación proactiva de amenazas y vulnerabilidades en los entornos de SDN. Esto se justifica por la necesidad de abordar las amenazas emergentes en SDN y garantizar la seguridad de la red y la disponibilidad del servicio. Este estudio se basa en una revisión de la literatura y destaca la importancia de los algoritmos de aprendizaje automático, para mejorar la detección de intrusiones en entornos SDN. La implementación de IA en la seguridad de SDN va más allá de detectar amenazas y proteger eficazmente los recursos y servicios de la red. Este es un elemento clave para garantizar la resiliencia y confiabilidad de SDN en un entorno de amenazas cibernéticas en constante evolución.

Palabras Claves: SDN, Inteligencia Artificial, Detección de Intrusiones, Ciberseguridad, Aprendizaje Automático, Arquitectura SDN, Aprendizaje profundo, Controlador SDN, Vulnerabilidades de SDN, OpenFlow, Centralización de Control.

SUMMARY

Software Defined Networking (SDN) represents an innovation in network management by providing significant flexibility and efficiency in its operation. However, this flexibility and efficiency also brings with it significant security challenges. The steady increase in cyber threats has become a serious concern, especially due to the centralized architecture of SDN, which relies on logical controllers to monitor data flows throughout the network. The proposed solution includes the application of artificial intelligence (AI) in attack mitigation, leveraging the ability to analyze data and detect anomalous patterns in real time, this involves proactively identifying threats and vulnerabilities in SDN environments. This is justified by the need to address emerging threats in SDN and ensure network security and service availability. This study is based on a literature review and highlights the importance of machine learning algorithms, to improve intrusion detection in SDN environments. Implementing AI in SDN security goes beyond detecting threats and effectively protecting network resources and services. This is a key element to ensure the resilience and reliability of SDN in a constantly evolving cyber threat e environment.

Keywords: SDN, Artificial Intelligence, Intrusion Detection, Cybersecurity, Machine Learning, SDN Architecture, Deep Learning, SDN Controller, SDN Vulnerabilities, OpenFlow, Control Centralization.

Contenido

Planteamiento del problema 8

Justificación 9

Objetivos del estudio 11

Objetivo general 11

Línea de investigación 12

Articulación del tema 13

Marco conceptual 14

Definición y Conceptos Básicos de SDN 14

Plano de Control (Control Plane) 14

Plano de Datos (Data Plane) 15

Controlador SDN (SDN Controller) 15

Dispositivos Programables (Switches y Enrutadores SDN) 16

Protocolo de Comunicación (OpenFlow) 16

Abstracción de la Red (Network Abstraction) 17

Arquitectura y Componentes de una Red SDN 17

Controlador SDN 18

Dispositivos de Red Programables 18

Interfaz Sur (Southbound Interface) 18

Interfaz Norte (Northbound Interface) 19

Ventajas y Desafíos de la Implementación de SDN 19

Ventajas de SDN 19

Desafíos de SDN 20

Ciberseguridad en Redes SDN: Amenazas y Vulnerabilidades Específicas 20

Ataques al Controlador SDN 21

Inyección de Flujos Maliciosos 21

Falsificación de Identidad 22

Ataques de Reenvío Malicioso 22

Exposición de API no Seguras 22

Escalada de Privilegios 23

Ataques de Reconocimiento 23

Riesgos asociados a la centralización del control en SDN 24

Punto Único de Fallo (Single Point of Failure) 24

Vulnerabilidad del Controlador 24

Ataques de Falsificación 24

Sobrecarga del Controlador 25

Desafíos de seguridad en la administración y configuración de SDN 25

Detección de Intrusiones 26

Relevancia de la Detección de Intrusiones 27

Métodos Tradicionales de Detección de Intrusiones en Redes 28

Detección de Firmas 28

Detección de Anomalías 28

Detección de Comportamiento Malicioso 29

Inteligencia Artificial (IA) en Ciberseguridad 29

Detección de Amenazas Avanzadas 29

Análisis de Comportamiento del Usuario 29

Detección de Malware y Ataques de Ingeniería Social 30

Gestión de Incidentes y Respuesta Automatizada 30

Predicción de Amenazas Futuras 30

Mejora de la Autenticación Biométrica 30

Análisis de Datos en Tiempo Real 30

Aprendizaje Automático y Aprendizaje Profundo en la Detección de Amenazas 31

Detección de Anomalías 31

Detección de Malware 31

Predicción de Amenazas 31

Aprendizaje Profundo en la Detección de Amenazas 32

Detección de Amenazas Avanzadas 32

Algoritmos de Aprendizaje Automático 33

Máquinas de Vectores de Soporte (SVM) 33

Redes Neuronales Convolucionales (CNN) 34

Redes Neuronales Recurrentes (RNN) 34

Bosques de Aislamiento 35

SVM de Una Clase 36

Algoritmos de Clustering 36

Reglas de Asociación 36

Bayesiano ingenuo 37

El árbol de decisiones 37

k-Nearest Neighbors 38

Algoritmo de Bosque Aleatorio 38

Marco metodológico 39

Resultados 40

Discusión de resultado 49

Conclusiones 51

Recomendaciones 53

Bibliografía 54

ANEXOS 58

Planteamiento del problema

En el campo del monitoreo y gestión de redes, las redes definidas por software surgen recientemente como una opción prometedora. Su capacidad para proporcionar flexibilidad, escalabilidad y eficiencia marca un contraste notable con los enfoques convencionales de redes. A pesar de las cualidades elogiables que definen estas propuestas, es innegable que también presentan desafíos de una magnitud sin precedentes. Esto se vuelve especialmente evidente al considerar áreas cruciales como la seguridad y la protección contra intrusiones no deseadas.

La importancia de proteger las redes definidas por software (SDN) crece constantemente, una razón clave es el aumento de las amenazas cibernéticas y la sofisticación de los ataques, ya que con la arquitectura centralizada de esta red y la dependencia de controladores lógicos crea vulnerabilidades que permiten a los atacantes comprometer la seguridad, esto puede hacer que la información se vea comprometida. Los métodos tradicionales de defensa pueden no ser suficientes para combatir estas nuevas amenazas. Encontrar formas de detectar ataques temprano es fundamental para mantener la seguridad de la red.

Cuando se produce interferencia en las redes definidas por software las consecuencias pueden ser devastadoras, los atacantes pueden aprovechar las vulnerabilidades del software y los protocolos para obtener acceso, manipular datos o incluso suspender servicios.

La inteligencia artificial actualmente está revolucionando el mundo de la seguridad informática. En las redes definidas por software (SDN), esta tecnología puede ayudar a analizar grandes volúmenes de datos, puede usar su capacidad para identificar patrones anómalos de manera eficiente lo que le permitiría tomar decisiones en tiempo real, contribuyendo así a la protección en contra de actividades maliciosa.

Justificación

Los entornos SDN, son un nuevo paradigma que se están utilizando en las redes, es por esta razón que existen nuevas amenazas a estas redes especialmente las relacionadas con las intrusiones. Es debido a esto que es necesario investigar los mecanismos que se pueden implementar para mitigar estos riesgos y garantizar la seguridad de las redes definidas por software.

En la actualidad, la tecnología se encuentra ante la constante presión de las ciberamenazas. Esta situación está generando la necesidad importante de adoptar enfoques cada vez más avanzados para lograr la detección inmediata y en tiempo real de posibles intrusos. La factibilidad de una reacción instantánea y automatizada ante las amenazas insinúa que esta fusión tecnológica no solo se limitaría a la detección de incidentes, sino que también podría contrarrestarlos en tiempo real. Esta unión de tecnologías podría fortalecer la seguridad en las redes y marcar un punto importante en cómo enfrentamos y prevenimos los desafíos cibernéticos actuales.

La evolución de las Redes Definidas por Software (SDN) han permitido transformar la manera en que se diseñan y gestionan las redes. Al separar el plano de control del plano de datos, las redes definidas por software proporcionan mayor flexibilidad y rapidez en la configuración y administración de la red. Esta innovación está siendo adoptada rápidamente en diversas industrias. Sin embargo, el cambio de estas redes trae consigo nuevas amenazas y problemas de seguridad. A medida que las redes se vuelven más dinámicas y programables, el riesgo de intrusiones y ataques a la red puede volverse más complejo y perturbador.

Al abordar esta problemática se busca mejorar la seguridad y confiabilidad de los entornos de las redes definidas por software. La idea clave aquí es utilizar técnicas innovadoras con la inteligencia artificial para detectar y prevenir ataques. Esto tiene un propósito importante, salvaguardar los recursos de la red y asegurar que los servicios que se ofrecen sigan siendo integrales y disponibles.

Objetivos del estudio

Objetivo general

Establecer los mecanismos para la detección de intrusiones en los entornos de redes definidas por software (SDN).

Objetivos específicos

- Identificar las amenazas y vulnerabilidades que están expuestos en los entornos de redes definidas por software SDN.
- Analizar los algoritmos de aprendizaje automático que pueden aplicarse para la detección de ataques en los entornos de redes definidas por software SDN.
- Establecer los algoritmos de aprendizaje automático que ayudarían a identificar patrones de ataques en entornos de redes definidas por software SDN.

Línea de investigación

Este estudio de caso se relaciona con la línea de investigación Sistemas de información y comunicación, emprendimiento e innovación al aplicar tecnologías inteligentes en la seguridad de las redes, y al ofrecer oportunidades para el desarrollo de soluciones innovadoras en el ámbito de la seguridad informática.

La sublínea de investigación Redes y tecnología inteligentes de software y hardware está estrechamente relacionada con el tema al explorar como la tecnología inteligente y las redes definidas por software pueden colaborar. La investigación en esta sublínea aborda la optimización y la eficacia de las redes modernas, lo que converge con el estudio de caso en cómo la inteligencia artificial puede mejorar la detección de intrusiones en el contexto específico de las redes definidas por software para fortalecer la seguridad en estos entornos dinámicos y programables.

Articulación del tema

Este estudio de caso sobre "La inteligencia artificial en la detección de intrusiones en entornos de redes definidas por software (SDN)" se convierte en un componente esencial. Las SDN representan una infraestructura fundamental para la gestión de redes modernas, pero también presentan desafíos significativos en términos de seguridad cibernética debido a su arquitectura centralizada y la necesidad de una supervisión constante.

En un mundo más digital, la seguridad de las redes y la información es muy importante. La inteligencia artificial (IA) es clave para proteger las redes SDN en el sector público y privado. La IA analiza muchos datos en tiempo real, detecta comportamientos extraños y alerta sobre posibles amenazas, lo que es vital para mantener seguros nuestros sistemas en estos entornos importantes.

La guía de los profesores es fundamental para implementar de manera segura las tecnologías de la información y comunicación. Los docentes no solo pueden proporcionar orientación y conocimientos especializados sobre la aplicación de la IA en la detección de intrusiones, sino que también pueden contribuir a la formación de profesionales capaces de enfrentar los desafíos de la ciberseguridad en las SDN.

Marco conceptual

Definición y Conceptos Básicos de SDN

Las Redes Definidas por Software (SDN, por sus siglas en inglés, Software-Defined Networking) representan una revolución en la forma en que se diseñan, administran y operan las redes de comunicación. En su esencia, SDN es un enfoque que busca separar el plano de control de una red del plano de datos, permitiendo una gestión más centralizada y programable. SDN, promueve la innovación porque introduce el concepto de programabilidad en el plano de datos. La arquitectura de SDN es diseñado en la separación por capas del plano de control y de datos (Mejía, Gonzales, Fernández, & Crespo, 2022).

Las Redes Definidas por Software (SDN) marcan un hito en la evolución de las redes de comunicación, al separar el plano de control del plano de datos. Esta separación es clave para lograr una gestión centralizada y programable de la red. En lugar de tomar decisiones de enrutamiento en dispositivos de red individuales, SDN permite que un controlador lógico central tome estas decisiones de manera más eficiente y dinámica. Esta innovación redefine la forma en que concebimos y operamos las redes, brindando mayor flexibilidad y control.

Plano de Control (Control Plane)

En una red convencional, el plano de control es el encargado de tomar decisiones sobre cómo se deben enrutar los datos. Estas decisiones se basan en protocolos de enrutamiento y reglas configuradas en los dispositivos de red. En SDN, el plano de control se separa físicamente de los dispositivos de red y se centraliza en un controlador lógico (Ruipérez, 2021).

El plano de control, que solía estar disperso en dispositivos de red, es ahora centralizado en un controlador SDN. Esta centralización simplifica la gestión y permite una toma de decisiones de enrutamiento más coherente y dinámica. Los protocolos de enrutamiento y las reglas de configuración que antes se ejecutaban en dispositivos de red individuales ahora son gestionados de manera unificada por el controlador. Esta separación de funciones es fundamental para la agilidad y la adaptabilidad de la red SDN.

Plano de Datos (Data Plane)

El plano de datos es la parte de la red que se encarga de transmitir los datos según las instrucciones proporcionadas por el plano de control. Los dispositivos de red en el plano de datos siguen las políticas y rutas definidas por el controlador SDN (Oviedo, Zhuma, Bowen, & Patiño, 2021).

Esta separación de funciones permite una mayor eficiencia y coherencia en la transmisión de datos. Los dispositivos en el plano de datos se convierten en ejecutores de las decisiones tomadas por el controlador, lo que facilita la gestión y la adaptación de la red a las necesidades cambiantes.

Controlador SDN (SDN Controller)

Según Williams Nicolalde (2021) El controlador es el componente central en una red SDN. Es un software que proporciona una vista global y unificada de la red, toma decisiones de enrutamiento y configura los dispositivos en el plano de datos para seguir esas decisiones. Los controladores pueden ser de código abierto o propietarios y son esenciales para la implementación de SDN.

Son el "cerebro" que dirige la red, permitiendo una gestión más eficiente y adaptativa. El controlador SDN es la piedra angular que hace posible la gestión centralizada y programable de una red definida por software.

Dispositivos Programables (Switches y Enrutadores SDN)

Los dispositivos de red en una arquitectura SDN son programables y obedecen las instrucciones del controlador. Estos dispositivos pueden ser reconfigurados en tiempo real, lo que permite una adaptación ágil a las necesidades cambiantes de la red (Alava & Paladines, 2020).

Esto significa que pueden ser reconfigurados en tiempo real, lo que habilita una adaptación ágil y dinámica de la red a medida que las demandas cambian. Esta característica es fundamental para permitir la gestión centralizada y programable que define a SDN y facilita la creación de redes altamente eficientes y adaptables.

Protocolo de Comunicación (OpenFlow)

OpenFlow es un protocolo de comunicación estándar utilizado para la comunicación entre el controlador SDN y los dispositivos de red. Permite que el controlador envíe instrucciones a los dispositivos y reciba información sobre el estado de la red (Becci, Morandi, & Marrone, 2020).

OpenFlow se ha convertido en un estándar esencial en el mundo de SDN, ya que proporciona un medio coherente y estandarizado para la toma de decisiones y la gestión de la red. Su adopción generalizada ha contribuido significativamente a la interoperabilidad y la eficiencia en las redes SDN.

Abstracción de la Red (Network Abstraction)

SDN proporciona una abstracción de la red que permite a los administradores de red verla de manera más simple y lógica, independientemente de la complejidad física subyacente (Alava & Paladines, 2020).

La abstracción de la red es una característica poderosa de SDN que simplifica la visualización y gestión de la red. Proporciona a los administradores de red una vista más simple y lógica de la red, independientemente de la complejidad física subyacente. Esto significa que pueden diseñar, configurar y gestionar la red de una manera más intuitiva y eficiente. La abstracción de la red desacopla la visión de la red de su implementación física, lo que facilita la implementación de políticas de red y la toma de decisiones basadas en necesidades operativas y comerciales en lugar de complejidades técnicas.

Los SDN se basan en la idea de desacoplar el control de la red de los dispositivos de red, lo que facilita una gestión más centralizada y programable. Esto brinda flexibilidad y agilidad en la configuración y operación de la red, lo que es esencial para enfrentar los desafíos actuales en ciberseguridad y adaptación a las demandas cambiantes de las aplicaciones y servicios.

Arquitectura y Componentes de una Red SDN

La arquitectura de una Red Definida por Software (SDN) se caracteriza por su capacidad para separar el plano de control del plano de datos, lo que permite una gestión más flexible y eficiente de la red (Moreno, 2019).

Esta arquitectura revoluciona la forma en que las decisiones de enrutamiento y políticas de red se implementan y gestionan. Al desacoplar el control de los dispositivos de red, SDN

permite una adaptación ágil a las cambiantes necesidades de la red, lo que es esencial en un mundo cada vez más dinámico y orientado hacia la automatización.

Controlador SDN

Como se mencionó previamente, el controlador SDN es el núcleo de la arquitectura. Este componente centralizado es responsable de tomar decisiones de enrutamiento y políticas de red. Los controladores SDN pueden ser de código abierto (por ejemplo, OpenDaylight, ONOS) o propietarios (como Cisco Application Centric Infrastructure, ACI) (Dairon, 2020).

Ya sea de código abierto o propietario, el controlador juega un papel esencial en la gestión y configuración de la red. Su capacidad para comunicarse con dispositivos de red programables y aplicaciones a través de interfaces definidas lo convierte en un facilitador clave para la toma de decisiones y la implementación de políticas en la red SDN.

Dispositivos de Red Programables

Estos dispositivos, como switches y enrutadores SDN, son controlados por el controlador y ejecutan instrucciones específicas. Son programables y pueden adaptarse a cambios en la red en tiempo real. Utilizan protocolos como OpenFlow para comunicarse con el controlador (Manrique, 2021).

Su programabilidad es fundamental para permitir una gestión centralizada y dinámica. La comunicación a través de protocolos como OpenFlow facilita la coordinación entre el controlador y estos dispositivos, lo que resulta en una red altamente adaptable y eficiente.

Interfaz Sur (Southbound Interface)

Es la interfaz de comunicación entre el controlador y los dispositivos de red. A través de esta interfaz, el controlador envía instrucciones de configuración y obtiene información sobre el estado de la red (Luz, 2022).

Esta comunicación bidireccional permite que el controlador ejerza un control preciso sobre los dispositivos de red programables y asegura que la red se ajuste continuamente a las políticas y necesidades definidas.

Interfaz Norte (Northbound Interface)

Esta interfaz permite que las aplicaciones y servicios se comuniquen con el controlador. Las aplicaciones pueden solicitar servicios de red y recibir información sobre la topología y el estado de la red (Lima. & Gavin, 2019).

Esta interfaz habilita la creación de aplicaciones y servicios personalizados que pueden aprovechar la flexibilidad y el control centralizado de SDN para abordar necesidades específicas en la gestión de la red.

Ventajas y Desafíos de la Implementación de SDN

Según Alexandra Jurado (2018) las ventajas de SDN son:

Ventajas de SDN

- **Flexibilidad y Agilidad:** SDN permite la configuración y reconfiguración rápida de la red en función de las necesidades cambiantes. Esto facilita la implementación de políticas de red dinámicas y la adaptación a las demandas de aplicaciones y servicios.
- **Centralización del Control:** La centralización del control en un controlador SDN proporciona una vista global de la red, lo que facilita la toma de decisiones coordinadas y una gestión más eficiente.

- **Optimización de Recursos:** SDN permite una utilización más eficiente de los recursos de red al ajustar dinámicamente el enrutamiento y la asignación de ancho de banda según sea necesario.
- **Automatización:** La programabilidad de SDN permite la automatización de tareas de red, lo que reduce la carga administrativa y minimiza los errores humanos.

Desafíos de SDN

- **Seguridad:** La centralización del control en SDN crea un punto único de fallo y aumenta la importancia de la seguridad del controlador. Se deben implementar medidas de seguridad robustas para proteger la red SDN contra intrusiones.
- **Escalabilidad:** El crecimiento de la red SDN puede plantear desafíos de escalabilidad en términos de capacidad del controlador y rendimiento de los dispositivos de red.
- **Interoperabilidad:** La interoperabilidad entre diferentes controladores y dispositivos de red puede ser un desafío, ya que no todos los componentes SDN siguen los mismos estándares.
- **Costos Iniciales:** La implementación de SDN puede requerir inversiones significativas en hardware y software, lo que puede ser un obstáculo para algunas organizaciones.

Ciberseguridad en Redes SDN: Amenazas y Vulnerabilidades Específicas

Las Redes Definidas por Software (SDN) ofrecen ventajas significativas en términos de flexibilidad y eficiencia de la red, pero también introducen amenazas y vulnerabilidades

específicas que deben abordarse de manera proactiva para garantizar la seguridad de la infraestructura de red (Becci, Morandi, & Marrone, 2019).

Abordar estas amenazas de manera proactiva es fundamental para garantizar la seguridad de la infraestructura de red en un entorno SDN. La capacidad de gestionar de forma centralizada la red a través del controlador SDN también significa que la seguridad de este componente es crítica.

Ataques al Controlador SDN

Dado que el controlador SDN es el componente central de la red, es un objetivo atractivo para los atacantes. Un ataque exitoso al controlador podría comprometer toda la red. Esto incluye ataques de denegación de servicio (DoS) dirigidos al controlador para interrumpir su funcionamiento o ataques de inundación de solicitudes maliciosas para sobrecargarlo. La seguridad del controlador es fundamental para proteger toda la red SDN, ya que un ataque exitoso podría comprometer todo el ecosistema (Cobos, 2021).

Inyección de Flujos Maliciosos

Los atacantes pueden intentar inyectar flujos de tráfico malicioso en la red SDN. Esto puede incluir la manipulación de tablas de flujo en dispositivos de red para dirigir el tráfico hacia ubicaciones no autorizadas o para llevar a cabo ataques de intermediario (Man-in-the-Middle) (Bone, Rodríguez, Sosa, & Núñez, 2021).

Los atacantes pueden intentar inyectar flujos de tráfico malicioso en una red SDN. Esto implica manipular las tablas de flujo en dispositivos de red para dirigir el tráfico hacia ubicaciones no autorizadas o para llevar a cabo ataques de intermediario, como el conocido

"Man-in-the-Middle". Estos ataques pueden tener graves consecuencias, ya que pueden desviar el tráfico legítimo a ubicaciones controladas por atacantes o interceptar datos confidenciales.

Falsificación de Identidad

La falta de autenticación sólida en algunos entornos SDN puede dar lugar a la falsificación de identidad. Los atacantes pueden hacerse pasar por controladores legítimos o dispositivos de red, lo que les permite tomar el control de la red y ejecutar ataques. La autenticación sólida es esencial para garantizar la integridad de la red y prevenir que los atacantes asuman identidades falsas para fines maliciosos (Incio, y otros, 2022).

Ataques de Reenvío Malicioso

En SDN, la gestión de flujos se realiza centralmente a través del controlador. Los atacantes pueden utilizar esta centralización para realizar ataques de reenvío malicioso, donde los flujos de tráfico se redirigen a ubicaciones no deseadas (Guzmán, 2022).

Los ataques de reenvío malicioso son un ejemplo de cómo los atacantes pueden aprovechar esta centralización. Mediante la manipulación de flujos de tráfico, los atacantes pueden redirigir datos a ubicaciones no deseadas, lo que puede interrumpir la operación normal de la red o exponer datos sensibles. La detección y prevención de estos ataques son fundamentales para mantener la seguridad de una red SDN.

Exposición de API no Seguras

Las interfaces de programación de aplicaciones (API) utilizadas para comunicarse con el controlador deben estar bien protegidas. Las API no seguras pueden ser explotadas por atacantes para acceder y controlar el controlador SDN (Cobos, 2021).

Los atacantes pueden explotar vulnerabilidades en estas API para acceder al controlador y, en última instancia, controlar la red. La seguridad de las API es esencial para prevenir accesos no autorizados y asegurar que solo aplicaciones legítimas puedan interactuar con el controlador.

Escalada de Privilegios

Los ataques de escalada de privilegios pueden permitir que los atacantes ganen acceso a funciones o áreas de la red a las que normalmente no tendrían acceso. Esto podría llevar a la manipulación de la red o al robo de datos confidenciales. La protección contra la escalada de privilegios es crítica para mantener la integridad y la seguridad de la red (Mejía, Gonzales, Fernández, & Crespo, 2022).

Ataques de Reconocimiento

Los atacantes pueden llevar a cabo escaneos de la red SDN para identificar dispositivos, controladores y posibles vulnerabilidades. Estos ataques de reconocimiento pueden ser el primer paso para un ataque más amplio.

Los atacantes a menudo comienzan con ataques de reconocimiento para identificar dispositivos, controladores y posibles vulnerabilidades en una red SDN. Estos escaneos de red les permiten planificar ataques más específicos y dirigidos. Detectar y responder a los ataques de reconocimiento es esencial para prevenir intrusiones posteriores y proteger la red contra amenazas (Moreno, 2019).

Para abordar estas amenazas y vulnerabilidades específicas en redes SDN, es esencial implementar prácticas de ciberseguridad sólidas. Esto incluye la autenticación y autorización adecuadas, la segmentación de la red para limitar la superficie de ataque, la monitorización constante de la red en busca de actividades sospechosas y la actualización regular de los componentes SDN para abordar las vulnerabilidades conocidas. Además, la implementación de

soluciones de detección y respuesta ante incidentes (IDS/IPS) puede ayudar a detectar y mitigar amenazas en tiempo real.

Riesgos asociados a la centralización del control en SDN

La centralización del control en SDN es una característica fundamental que permite una administración más eficiente y una toma de decisiones coordinada. Sin embargo, esta centralización también introduce ciertos riesgos que deben ser cuidadosamente considerados (Incio, y otros, 2022).

Punto Único de Fallo (Single Point of Failure)

Dado que el controlador SDN es el componente centralizado que toma decisiones críticas para la red, cualquier interrupción o compromiso del controlador puede afectar toda la red. Los ataques exitosos al controlador pueden causar una interrupción total o parcial de la red (Nicolalde, 2021).

Vulnerabilidad del Controlador

Los controladores SDN pueden ser vulnerables a ataques, especialmente si no se implementan adecuadas medidas de seguridad. Los ataques dirigidos al controlador, como los de denegación de servicio (DoS) o los intentos de escalada de privilegios, pueden ser perjudiciales (Luz, 2022).

Ataques de Falsificación

Dado que el controlador toma decisiones basadas en la información que recibe de los dispositivos de red, los ataques de falsificación de información pueden ser un riesgo. Los atacantes pueden enviar información falsa al controlador para manipular el enrutamiento de tráfico.

Sobrecarga del Controlador

En redes SDN de gran escala, la carga en el controlador puede ser significativa. El procesamiento de numerosas solicitudes y la gestión de flujos de datos pueden llevar a una sobrecarga, lo que afecta negativamente la eficiencia y la capacidad de respuesta de la red (Manrique, 2021).

Desafíos de seguridad en la administración y configuración de SDN

La administración y configuración de una red SDN plantean desafíos específicos relacionados con la seguridad que deben abordarse adecuadamente:

- **Gestión de Credenciales:** La gestión de credenciales de acceso a componentes SDN, como el controlador, es esencial para prevenir el acceso no autorizado. La gestión débil de contraseñas o la falta de autenticación de dos factores pueden dejar la red vulnerable.
- **Control de Acceso:** La administración de políticas de control de acceso es fundamental. Garantizar que solo usuarios autorizados tengan acceso a funciones y recursos críticos es esencial para prevenir ataques internos.
- **Actualizaciones y Parches:** Mantener los componentes SDN actualizados con las últimas correcciones de seguridad es un desafío constante. La falta de actualizaciones o parches puede dejar la red vulnerable a vulnerabilidades conocidas.
- **Monitorización Continua:** La monitorización en tiempo real de la red SDN es crucial para detectar actividades sospechosas o intentos de intrusión. La falta de una solución de monitorización adecuada puede llevar a la detección tardía de amenazas.

- **Gestión de Políticas de Seguridad:** La implementación y gestión de políticas de seguridad coherentes en toda la red SDN es esencial. Esto incluye la definición de políticas de firewall y reglas de enrutamiento seguras.

La centralización del control en SDN introduce riesgos asociados con la vulnerabilidad del controlador y ataques de falsificación, mientras que la administración y configuración de SDN plantean desafíos específicos relacionados con la gestión de credenciales, el control de acceso y la monitorización continua. La seguridad en SDN debe abordarse de manera integral para mitigar estos riesgos y desafíos (Lima. & Gavin, 2019).

Detección de Intrusiones

La detección de intrusiones (IDS, por sus siglas en inglés, Intrusion Detection System) es un componente crítico de la seguridad cibernética que se utiliza para identificar y responder a posibles amenazas y actividades maliciosas en una red o sistema informático. El concepto fundamental de la detección de intrusiones implica el monitoreo continuo y la evaluación de eventos y actividades en busca de patrones anómalos que puedan indicar una intrusión o actividad no autorizada (Alava & Paladines, 2020).

La detección de intrusiones se basa en la premisa de que las actividades maliciosas o las intrusiones en una red o sistema informático generan patrones de comportamiento diferentes a los eventos normales. Un IDS analiza el tráfico de red, los registros del sistema y otros datos relevantes para identificar estos patrones anómalos. Cuando se detecta una actividad sospechosa, el IDS puede generar alertas, tomar medidas de mitigación o informar a los administradores de la red para que tomen medidas correctivas.

Relevancia de la Detección de Intrusiones

La relevancia de la detección de intrusiones en la seguridad cibernética moderna es innegable y está en constante aumento debido a varios factores:

- **Aumento de las Amenazas Cibernéticas:** En un entorno cibernético en constante evolución, las amenazas cibernéticas y los ataques maliciosos son cada vez más sofisticados y diversificados. Los ciberdelincuentes están constantemente desarrollando nuevas tácticas y herramientas para comprometer la seguridad de las redes y sistemas.
- **Protección de Datos Sensibles:** Las organizaciones almacenan y gestionan grandes cantidades de datos sensibles, desde información personal y financiera hasta propiedad intelectual. La detección de intrusiones es esencial para proteger estos datos y prevenir su acceso no autorizado o su robo.
- **Cumplimiento Normativo:** Muchas industrias y organizaciones están sujetas a regulaciones estrictas que requieren la implementación de medidas de seguridad cibernética, incluida la detección de intrusiones. El incumplimiento de estas regulaciones puede resultar en sanciones graves.
- **Respuesta Rápida a Incidentes:** La detección de intrusiones permite una respuesta rápida y efectiva a incidentes de seguridad. La identificación temprana de una amenaza cibernética puede ayudar a minimizar el impacto y las consecuencias de un ataque.
- **Mejora de la Postura de Seguridad:** La implementación de un IDS no solo ayuda a detectar intrusiones, sino que también contribuye a mejorar la postura

general de seguridad de una organización. El conocimiento de las amenazas y vulnerabilidades permite tomar medidas proactivas para fortalecer la seguridad.

La detección de intrusiones desempeña un papel crítico en la protección de las redes y sistemas contra amenazas cibernéticas. Su capacidad para identificar patrones anómalos y posibles intrusiones es esencial para mantener la seguridad en un entorno cibernético en constante cambio y cada vez más peligroso. La inversión en tecnologías y prácticas de detección de intrusiones es esencial para garantizar la integridad y confidencialidad de los datos y la continuidad de las operaciones comerciales (Oviedo, Zhuma, Bowen, & Patiño, 2021).

Métodos Tradicionales de Detección de Intrusiones en Redes

Los métodos tradicionales de detección de intrusiones en redes han sido fundamentales para proteger la seguridad de los sistemas informáticos durante muchos años. Estos métodos se basan en la observación y análisis de patrones de tráfico y comportamiento de la red para identificar actividades maliciosas o anómalas (Dairon, 2020).

Detección de Firmas

Este enfoque se basa en la creación y el uso de firmas o patrones conocidos de ataques. Los sistemas de detección de intrusiones (IDS) con bases de datos de firmas comparan el tráfico de red con estas firmas y generan alertas cuando se encuentra una coincidencia. Sin embargo, este método es efectivo solo para ataques previamente identificados y no puede detectar nuevas amenazas (Jurado, 2018).

Detección de Anomalías

La detección de anomalías se centra en identificar comportamientos inusuales en la red. Los sistemas de detección de intrusiones basados en anomalías establecen un perfil del tráfico normal y generan alertas cuando se observan desviaciones significativas de ese perfil. Esto puede

ser efectivo para detectar amenazas desconocidas, pero puede generar falsos positivos (Mejía, Gonzales, Fernández, & Crespo, 2022).

Detección de Comportamiento Malicioso

Este método se enfoca en el comportamiento de los usuarios y sistemas en la red. Busca identificar actividades maliciosas, como intentos repetidos de inicio de sesión fallidos o accesos no autorizados a recursos. Los sistemas de detección de comportamiento malicioso pueden ser efectivos para detectar amenazas internas (Moreno, 2019).

Inteligencia Artificial (IA) en Ciberseguridad

La incorporación de la Inteligencia Artificial (IA) en la ciberseguridad ha transformado radicalmente la forma en que se abordan las amenazas cibernéticas. La IA, con su capacidad para aprender de datos y tomar decisiones en tiempo real, ha demostrado ser una herramienta poderosa para identificar y mitigar riesgos de seguridad. Aquí exploramos algunas de las aplicaciones clave de la IA en ciberseguridad (Alava & Paladines, 2020).

Detección de Amenazas Avanzadas

La IA se utiliza para identificar amenazas cibernéticas avanzadas que pueden pasar desapercibidas para los sistemas tradicionales de detección de intrusiones. Los algoritmos de IA pueden analizar grandes volúmenes de datos, identificar patrones de comportamiento anómalo y generar alertas tempranas sobre posibles amenazas (Becci, Morandi, & Marrone, 2019).

Análisis de Comportamiento del Usuario

La IA se utiliza para monitorear y analizar el comportamiento de los usuarios en una red. Puede identificar actividades inusuales o sospechosas, como intentos de inicio de sesión no autorizados o acceso a recursos sensibles, y generar alertas o tomar medidas de seguridad (Alava & Paladines, 2020).

Detección de Malware y Ataques de Ingeniería Social

Los sistemas de IA pueden analizar archivos y correos electrónicos en busca de malware y phishing. Pueden identificar patrones y características comunes de ataques de ingeniería social y ayudar a prevenir que los usuarios caigan en trampas (Becci, Morandi, & Marrone, 2019).

Gestión de Incidentes y Respuesta Automatizada

La IA se utiliza para automatizar la gestión de incidentes de seguridad. Puede tomar decisiones rápidas sobre la mitigación de amenazas, como la cuarentena de sistemas infectados o la desconexión de dispositivos comprometidos, sin intervención humana (Guzmán, 2022).

Predicción de Amenazas Futuras

La IA puede analizar tendencias y datos históricos para predecir amenazas cibernéticas futuras. Esto permite a las organizaciones tomar medidas proactivas para fortalecer su seguridad y prepararse para posibles ataques (Oviedo, Zhuma, Bowen, & Patiño, 2021).

Mejora de la Autenticación Biométrica

La IA se utiliza para mejorar la autenticación biométrica, como el reconocimiento facial o de voz. Esto aumenta la precisión y la seguridad de la autenticación, reduciendo el riesgo de acceso no autorizado (Moreno, 2019).

Análisis de Datos en Tiempo Real

La IA puede analizar datos en tiempo real de múltiples fuentes, incluidos registros de eventos de red y registros de sistemas, para identificar actividad sospechosa. Esto permite una respuesta más rápida a posibles amenazas (Cobos, 2021).

La IA desempeña un papel fundamental en la ciberseguridad al mejorar la detección de amenazas, la gestión de incidentes y la protección de datos. Sus aplicaciones abarcan desde la detección de malware hasta la autenticación biométrica y la predicción de amenazas futuras. La

IA permite una ciberseguridad más efectiva y adaptativa en un entorno cibernético en constante evolución.

Aprendizaje Automático y Aprendizaje Profundo en la Detección de Amenazas

El aprendizaje automático (Machine Learning, ML) y el aprendizaje profundo (Deep Learning, DL) son ramas de la inteligencia artificial que se han convertido en componentes esenciales de la ciberseguridad moderna (Manrique, 2021).

Estos enfoques de IA permiten a las organizaciones mejorar significativamente la detección y mitigación de amenazas cibernéticas mediante el análisis de datos de manera automatizada y precisa. El aprendizaje automático se basa en la capacidad de las máquinas para aprender patrones y tomar decisiones basadas en datos históricos y en tiempo real.

Detección de Anomalías

Los algoritmos de ML pueden aprender el comportamiento normal de una red o sistema y, cuando detectan desviaciones significativas de ese comportamiento, generan alertas de posibles amenazas (Alava & Paladines, 2020).

Detección de Malware

El ML se aplica para identificar archivos maliciosos o comportamientos sospechosos que pueden indicar la presencia de malware. Se pueden entrenar modelos para reconocer firmas de malware conocidas y comportamientos anómalos (Jurado, 2018).

Predicción de Amenazas

El ML puede analizar tendencias y datos históricos para prever amenazas futuras. Esto permite a las organizaciones tomar medidas proactivas para fortalecer su seguridad.

Aprendizaje Profundo en la Detección de Amenazas

El aprendizaje profundo es una subrama del aprendizaje automático que se basa en redes neuronales artificiales profundas. Su capacidad para analizar datos no estructurados y complejos lo hace especialmente efectivo en la ciberseguridad:

Detección de Amenazas Avanzadas

Las redes neuronales profundas pueden identificar patrones extremadamente complejos en los datos, lo que las hace adecuadas para la detección de amenazas altamente sofisticadas y avanzadas (Bone, Rodríguez, Sosa, & Núñez, 2021).

- **Procesamiento de Datos no Estructurados:** El aprendizaje profundo es capaz de analizar datos no estructurados, como el contenido de correos electrónicos o archivos multimedia, en busca de amenazas ocultas.
- **Mejora de la Autenticación Biométrica:** En la autenticación biométrica, las redes neuronales profundas se utilizan para el reconocimiento facial o de voz, mejorando la precisión y la seguridad.
- **Análisis de Comportamiento del Usuario:** Las redes neuronales profundas pueden identificar patrones de comportamiento del usuario que podrían indicar actividades maliciosas, como el robo de credenciales.

El aprendizaje automático y el aprendizaje profundo han revolucionado la ciberseguridad al permitir la detección de amenazas más precisa y eficiente. Estos enfoques de IA son fundamentales para identificar patrones anómalos, predecir amenazas futuras y mejorar la seguridad en un entorno cibernético en constante evolución. Su aplicación en la detección de amenazas es esencial para proteger sistemas y datos críticos contra ataques cibernéticos (Incio, y otros, 2022).

Algoritmos de Aprendizaje Automático

Los algoritmos de aprendizaje automático son un conjunto de técnicas y métodos que permiten a las computadoras aprender y mejorar su rendimiento en tareas específicas sin ser programadas explícitamente. En lugar de seguir instrucciones detalladas, las máquinas utilizan datos para reconocer patrones, tomar decisiones y adaptarse a diferentes situaciones (Rendón, 2020).

Máquinas de Vectores de Soporte (SVM)

Las Máquinas de Vectores de Soporte (SVM) son un conjunto de algoritmos de aprendizaje automático utilizados en una variedad de aplicaciones, incluida la detección de intrusiones en entornos de redes definidas por software (SDN). Su fundamento se basa en la búsqueda de un hiperplano óptimo que permita la clasificación precisa de datos en diferentes categorías. En términos más simples, las SVM buscan la mejor forma de dividir conjuntos de datos en clases, maximizando la distancia entre los puntos de datos de las diferentes clases y, al mismo tiempo, minimizando los errores de clasificación (Becci, Morandi, & Marrone, 2020).

En cuanto a la detección de intrusiones en entornos de redes definidas por software (SDN), las SVM se han convertido en una herramienta esencial debido a su capacidad para abordar problemas complejos de clasificación y detección de anomalías. A medida que las redes SDN continúan desempeñando un papel crucial en la infraestructura de comunicaciones moderna, la seguridad de estas redes se ha vuelto una preocupación primordial. Las SVM ofrecen una solución eficaz para abordar los desafíos de seguridad en estos entornos altamente dinámicos y cambiantes.

Redes Neuronales Convolucionales (CNN)

Las Redes Neuronales Convolucionales (CNN) son un tipo especializado de red neuronal artificial diseñada específicamente para procesar datos con una estructura de cuadrícula, como imágenes y, en el contexto de la detección de intrusiones en redes definidas por software (SDN), flujos de datos de tráfico de red. Estas redes han demostrado un gran éxito en tareas de visión por computadora y, en aplicaciones de seguridad cibernética, se han adaptado para analizar patrones y comportamientos en el tráfico de red con el objetivo de identificar intrusiones y amenazas (Mejía, Legarda, Agudelo, & Rebollar, 2021).

En el campo de la seguridad de redes definidas por software (SDN), las Redes Neuronales Convolucionales (CNN) se han convertido en una herramienta de vanguardia para la detección de intrusiones. A medida que las redes SDN se vuelven más complejas y dinámicas, la detección de amenazas cibernéticas se vuelve un desafío aún mayor. Las CNN ofrecen una solución eficaz para este desafío al permitir el análisis profundo y la identificación de patrones sutiles en el tráfico de red, lo que puede indicar actividades maliciosas.

Redes Neuronales Recurrentes (RNN)

Las Redes Neuronales Recurrentes (RNN) son un tipo de red neuronal artificial que se utiliza en el campo de la inteligencia artificial y el aprendizaje automático para procesar secuencias de datos. A diferencia de las redes neuronales convencionales, las RNN tienen conexiones recurrentes que les permiten tomar decisiones basadas en entradas anteriores, lo que las hace ideales para modelar datos secuenciales, como el tráfico de red en entornos de redes definidas por software (SDN) (Arana, 2021).

las Redes Neuronales Recurrentes (RNN) desempeñan un papel importante en el contexto de la detección de intrusiones en redes definidas por software (SDN). A medida que las

amenazas cibernéticas se vuelven más sofisticadas y evasivas, la capacidad de analizar el tráfico de red de manera secuencial y detectar patrones anómalos en tiempo real es esencial. Las RNN son especialmente adecuadas para esta tarea, ya que pueden capturar dependencias temporales en los datos de tráfico, lo que facilita la identificación de comportamientos maliciosos.

Bosques de Aislamiento

Los Bosques de Aislamiento (Isolation Forests) son una técnica de aprendizaje automático utilizada en la detección de anomalías y intrusiones en datos no estructurados o complejos. A diferencia de otros algoritmos, como las Máquinas de Vectores de Soporte (SVM) o las Redes Neuronales, los Bosques de Aislamiento se destacan por su capacidad para aislar observaciones anómalas de manera eficiente y efectiva. Están diseñados para identificar patrones raros y sospechosos en grandes conjuntos de datos, lo que los hace relevantes para la detección de intrusiones en entornos de redes definidas por software (SDN) (Incio, y otros, 2022).

En el contexto de la seguridad cibernética y la detección de intrusiones en redes definidas por software (SDN), los Bosques de Aislamiento desempeñan un papel importante al abordar gran volumen de datos ya que los bosques de aislamiento son eficientes en la detección de intrusiones en conjuntos de datos masivos, variedad de patrones de ataque y detección temprana.

En base a esto se especifica que son una herramienta poderosa en la detección de intrusiones en redes definidas por software (SDN) debido a su eficiencia en grandes conjuntos de datos, su capacidad para identificar anomalías sin etiquetas y su detección en tiempo real. Su aplicación mejora la seguridad cibernética al detectar patrones de ataque desconocidos y minimizar las falsas alarmas, lo que permite una respuesta más efectiva a las amenazas en entornos SDN en constante evolución.

SVM de Una Clase

Las Máquinas de Vectores de Soporte de Una Clase (One-Class Support Vector Machines o One-Class SVM) son un tipo especializado de algoritmo de aprendizaje automático que se utiliza en la detección de anomalías y la clasificación de datos en una sola clase. A diferencia de las SVM tradicionales que se utilizan para la clasificación binaria, las SVM de Una Clase están diseñadas específicamente para identificar patrones inusuales en un conjunto de datos y asignarlos a una sola clase, que generalmente representa la clase de "anomalía" (Guzmán, 2022).

Algoritmos de Clustering

Los algoritmos de clustering son una categoría de técnicas de aprendizaje automático utilizadas para agrupar datos en conjuntos o clústeres basados en la similitud entre sus características. Estos algoritmos buscan identificar patrones intrínsecos en los datos y agrupar elementos que son más similares entre sí en el mismo clúster (Rendón, 2020).

Reglas de Asociación

Las reglas de asociación son un conjunto de técnicas de aprendizaje automático que se utilizan para descubrir relaciones y patrones entre elementos de datos en conjuntos de datos transaccionales. Estas reglas identifican conexiones frecuentes entre elementos y generan asociaciones basadas en la coaparición de estos elementos (Alava & Paladines, 2020).

Bayesiano ingenuo

Un clasificador Bayesiano ingenuo, o "Naive Bayes", es un conjunto de algoritmos de aprendizaje supervisado que se utilizan para construir modelos predictivos para clasificaciones binarias o múltiples. Naive Bayes trabaja con probabilidades condicionales basadas en el teorema de Bayes, que son independientes entre sí, pero muestran la probabilidad de una clasificación basada en sus factores combinados (Fortune Business Insights, 2022).

Un clasificador ingenuo de Bayes basado en el teorema de Bayes puede ser una herramienta valiosa para las redes definidas por software (SDN) que ayuda con la clasificación y priorización de datos en tiempo real. Utilizando probabilidades condicionales independientes, este algoritmo puede analizar el tráfico de red y asignar tareas a diferentes clases de datos, lo que facilita la toma de decisiones inteligentes en el enrutamiento SDN y la gestión del ancho de banda**.**

El árbol de decisiones

Un árbol de decisión es un algoritmo de aprendizaje supervisado que se utiliza para clasificación y modelado predictivo. Al igual que un diagrama de flujo gráfico, un árbol de decisión comienza con un nodo raíz que hace a los datos una pregunta específica y la envía a una rama según la respuesta. Cada una de estas ramas conduce a un nodo interno, que a su vez hace a los datos una pregunta más antes de dirigirlos a otra rama según la respuesta. Esto continúa hasta que los datos llegan a un terminal, también llamado nodo hoja, que no se ramifica más. Los árboles de decisión son comunes en el aprendizaje automático porque pueden manejar conjuntos de datos complejos con relativa facilidad (Fortune Business Insights, 2022).

Los árboles de decisión, por otra parte, son valiosos para la toma de decisiones en tiempo real en redes definidas por software. Se pueden utilizar para crear políticas de seguridad basadas

en condiciones específicas del tráfico de la red, como la detección de patrones sospechosos o comportamientos anormales. Los nodos de decisión del árbol de decisión pueden hacer preguntas sobre el tráfico y determinar acciones apropiadas para mitigar las amenazas cibernéticas, contribuyendo a la seguridad de una red SDN.

k-Nearest Neighbors

Es un algoritmo de aprendizaje supervisado que se utiliza para clasificación y problemas de regresión. Se basa en analizar datos de los vecinos más cercanos para predecir un nuevo punto de datos. El factor de análisis más importante es el número de vecinos para un mejor rendimiento (Fortune Business Insights, 2022).

Los algoritmos K-Nearest Neighbor (KNN) también tienen aplicaciones en la seguridad de redes definidas por software. KNN se puede utilizar para identificar patrones de tráfico similares y agrupar flujos de datos con comportamiento anormal, lo que facilita la detección de amenazas.

Algoritmo de Bosque Aleatorio

El algoritmo de bosque aleatorio utiliza árboles de decisión para clasificación y modelado predictivo. En un bosque aleatorio, muchos árboles de decisión se entrenan utilizando una muestra aleatoria del conjunto de entrenamiento. Luego ingresan los mismos datos en cada árbol de decisión del bosque aleatorio y calculan los resultados finales. Luego se selecciona el resultado más frecuente como el más probable en el conjunto de datos (Fortune Business Insights, 2022).

Un algoritmo de bosque aleatorio que utiliza múltiples árboles de decisión proporciona mayor solidez para la detección de intrusiones en redes definidas por software. Al utilizar una combinación de árboles de decisión entrenados con muestras aleatorias, puede mejorar la

precisión de la detección de amenazas y reducir el riesgo de falsos positivos. Esto es particularmente útil en entornos SDN donde la adaptabilidad y la eficiencia en la detección de amenazas son esenciales.

Marco metodológico

Dado que este estudio se fundamenta en la recopilación de datos secundarios y el examen exhaustivo de la literatura preexistente, se optará por una aproximación de naturaleza cualitativa. Esto permite un análisis detallado de las relaciones y patrones en los datos sin necesidad de encuestas o entrevistas, brindando una comprensión profunda del tema.

Tipo de Investigación

Este estudio se inserta en el contexto de una investigación que combina elementos exploratorios y descriptivos. La parte exploratoria se enfoca en adentrarse en la comprensión exhaustiva de las amenazas y vulnerabilidades que acechan a los entornos de las redes definidas por software (SDN), destacando el papel esencial que la inteligencia artificial puede desempeñar en su identificación y mitigación. La investigación también tiene un componente descriptivo mediante el análisis de algoritmos de aprendizaje automático aplicables a SDN.

Técnicas e Instrumentos de recolección de Datos

El método de recolección de datos utilizados para llevar a cabo en esta investigación incluye el análisis documental y bibliográfico, este proceso busca recopilar información de una variedad de fuentes para obtener una comprensión completa y precisa del tema de investigación,

además de permitir un análisis sencillo de datos cualitativos para comprender la información obtenida.

Resultados

Esta investigación se basa en una descripción general de las redes definidas por software (SDN) y se centra en cómo la inteligencia artificial (IA) puede ayudar a prevenir ataques. En este contexto, se han identificado enfoques específicos para combatir amenazas como ataques a controladores SDN, reenvío malicioso, suplantación de identidad, exposición de API desprotegidas y ataques de reconocimiento.

Ataques al Controlador SDN

El algoritmo más adecuado para detectar y combatir ataques a controladores SDN es el de Bosques Aislados (Isolation Forests). Esta elección se basa en varias buenas razones, los bosques aislados son muy eficaces para detectar anomalías, lo cual es crucial para detectar ataques contra el controlador SDN porque pueden tener diferentes formas y ser de naturaleza inusual. Además, estos algoritmos no requieren identificadores específicos de ataques anteriores, lo que significa que pueden detectar patrones de ataque desconocidos y adaptarse a amenazas en constante evolución. Su capacidad para detectar patrones raros y sospechosos los hace ideales para la detección temprana de ataques al controlador SDN, lo que permite una respuesta a las amenazas más rápida y eficaz.

Comienza recopilando información sobre el comportamiento normal del controlador SDN, incluidas métricas de rendimiento, solicitudes y respuestas, eventos de red y más. Luego se seleccionan las características más importantes de estos datos para ayudar a identificar posibles ataques. Se crea un conjunto de datos de entrenamiento que incluye ejemplos de comportamiento típico del controlador y, cuando sea posible, ejemplos de ataques históricos o simulados. Se entrena un modelo de bosque de aislamiento en este conjunto de datos para aprender a reconocer patrones anormales en función de características seleccionadas. Este modelo se aplica para analizar el comportamiento en tiempo real de un controlador SDN, y cualquier variación significativa de los modelos convencionales puede activar alarmas o notificaciones para investigar posibles ataques. Además, el modelo se actualiza constantemente con nuevos datos para adaptarse a cambios en el comportamiento del responsable del tratamiento o la aparición de nuevos tipos de ataques, asegurando su eficacia en el tiempo.

Ataques de Reenvío Malicioso

La selección del algoritmo de aprendizaje automático idóneo para la detección de ataques de reenvío maliciosos en redes definidas por software (SDN) se convierte en un pilar estratégico de gran envergadura. En este contexto, las redes neuronales convolucionales (CNN) se erigen como una elección sobresaliente debido a su aptitud para descifrar patrones en los flujos de datos de tráfico de red.

Las redes neuronales convolucionales (CNN) exhiben una destacada eficacia en el análisis de datos con estructura de red, como los flujos de datos de tráfico de red en SDN. Su historial de éxito en el ámbito de la ciberseguridad las convierte en un recurso promisorio para contrarrestar la amenaza de los ataques de retransmisión maliciosa en las redes SDN.

El proceso de detección de estos ataques mediante el algoritmo CNN implica la captura meticulosa del tráfico de red y la recopilación de eventos de control procedentes de la red SDN, lo cual incluye información sobre flujos de tráfico, variaciones en las rutas de comunicación y eventos del controlador. Esta información es posteriormente sometida a una clasificación que distingue entre datos legítimos, representativos de un comportamiento normal, y datos sospechosos, indicativos de potenciales ataques de reenvío maliciosos.

A continuación, los datos atraviesan un proceso de preprocesamiento, el cual abarca pasos como la normalización, reducción de ruido y segmentación en fragmentos más pequeños, facilitando así la posterior fase de análisis. Tras ello, se procede a entrenar un modelo CNN utilizando el conjunto de datos previamente etiquetado. Este modelo adquiere la habilidad de identificar patrones y anomalías en los datos del tráfico de la red que puedan insinuar un ataque de redireccionamiento malicioso.

Una vez que el modelo CNN ha concluido su entrenamiento, se somete a una validación empleando datos adicionales que no formaron parte del proceso de formación. Este paso es crucial para calibrar y perfeccionar el modelo con el fin de incrementar su precisión y su capacidad de detección. Consecuentemente, el modelo se integra en un entorno SDN en tiempo real, con la misión de monitorizar el tráfico de la red en curso. En esta labor, analiza meticulosamente los flujos de tráfico entrantes y salientes, a la caza de patrones sospechosos que puedan denotar una amenaza de reenvío malicioso.

Cuando el modelo detecta actividad sospechosa que sugiere la presencia de un ataque de reenvío malicioso, se activan medidas inmediatas, que pueden incluir el bloqueo o la redirección del tráfico, alertas dirigidas a los administradores del sistema o la implementación de políticas de seguridad específicas.

Falsificación de Identidad

Para combatir la amenaza de la suplantación de identidad en redes definidas por software (SDN). Las máquinas de vectores de soporte (SVM) se distinguen por su capacidad para resolver problemas complejos de detección y clasificación de anomalías, lo que las convierte en una herramienta importante para la seguridad de la red SDN. La razón principal de esta elección es su capacidad para encontrar hiperplanos óptimos que permitan una clasificación precisa de los datos en diferentes clases maximizando la diferencia entre ellos.

El procedimiento para detectar la amenaza de falsificación de identidad con SVM involucra varias etapas clave, la información de autenticación y los registros de actividad se recopilan en la red SDN. Esta información incluye información sobre controladores, dispositivos de red y acciones tomadas. Además, se deben agregar etiquetas para indicar si la actividad o identidad es legítima o sospechosa.

Después de recopilar un conjunto de datos de entrenamiento con ejemplos de autenticación legítimos y potencialmente fraudulentos, se entrena el modelo SVM. El modelo aprende a trazar un límite de decisión que separa las identidades legítimas de las falsas en función de características relevantes como patrones de autenticación y registros de actividad.

Una vez entrenado el modelo, se utiliza continuamente para analizar operaciones de autenticación en tiempo real en una red SDN. Cualquier intento de fraude que el modelo SVM

identifique como sospechoso puede desencadenar una alarma o acción, como impedir el acceso no autorizado.

Ataques de Reenvío Malicioso

Cuando se trata de abordar el ataque del tráfico malicioso dirigido a redes definidas por software (SDN), el algoritmo de aprendizaje automático más idóneo es el de Bosques Aislados. Estos bosques destacan por su excepcional eficacia en la detección de anomalías, un elemento crucial para identificar flujos de datos maliciosos que, a menudo, adoptan formas inusuales en una red SDN. Además, su capacidad para identificar estas anomalías en una fase temprana se convierte en un elemento distintivo, permitiendo la implementación de medidas preventivas antes de que los ataques inflijan daños significativos.

El proceso de identificar una amenaza de flujo adverso mediante Bosques Aislados, se lleva a cabo la recopilación de información sobre el tráfico de red dentro de la infraestructura de SDN, lo que incluye detalles acerca de los flujos de tráfico, como su origen, destino, protocolo y puertos empleados. A continuación, se realiza una cuidadosa selección de las características clave de estos flujos de tráfico, características que pueden revelar indicios de flujos maliciosos, tales como patrones de comunicación poco comunes, alteraciones abruptas en el tráfico o modos de uso no autorizados.

Una vez creado un conjunto de datos de entrenamiento, que incorpora ejemplos de flujos de tráfico considerados normales y, preferentemente, ejemplos de flujos maliciosos previamente detectados o simulados, se procede a entrenar el modelo de Bosques Aislados. Este modelo

adquiere la habilidad de reconocer patrones anómalos basándose en las características previamente seleccionadas.

Una vez que el modelo se encuentra en estado entrenado, se despliega para llevar a cabo una vigilancia continua del tráfico en tiempo real dentro de una red SDN. Cualquier flujo de tráfico que el modelo considere anormal puede generar una alerta o desencadenar una acción de bloqueo para investigar la presencia de flujos maliciosos. Es importante destacar que el modelo de Bosques Aislados se mantiene actualizado de forma constante mediante la incorporación de nuevos datos de tráfico, lo cual le permite adaptarse a las modificaciones en el comportamiento de la red o la aparición de nuevos patrones de ataque, garantizando así su eficacia en el largo plazo**.**

Escalada de Privilegios

Elegir un algoritmo de aprendizaje automático eficaz es esencial para combatir los ataques de escalada de privilegios de redes definidas por software (SDN), la opción más adecuada sería utilizar máquinas de vectores de soporte de una clase (One-Class SVM).

Las máquinas de vectores de soporte de una clase (SVM de una clase) son una opción sólida porque pueden identificar patrones inusuales en un conjunto de datos y asignarlos a una sola clase, que generalmente representa una "anomalía". Esto significa que estas SVM son particularmente adecuadas para detectar comportamientos o actividades inusuales o no autorizados en una red SDN.

El procedimiento para identificar el ataque de escalada de privilegios se recopilan datos sobre la actividad y el rendimiento del usuario en la red SDN, que pueden incluir registros de acceso, registros de comandos ejecutados y eventos de seguridad. Luego se construye un

conjunto de datos etiquetado como "normal" para representar el comportamiento típico y autorizado en una red SDN. Este conjunto de datos se utiliza para entrenar un modelo SVM de una clase.

Después que el modelo haya sido entrenado, se utiliza para monitorear la actividad en la red SDN en tiempo real. Si detecta un comportamiento significativamente diferente al normal, generará una alarma. Por ejemplo, si un usuario intenta ejecutar comandos de configuración fuera de su alcance autorizado, como cambiar políticas de seguridad críticas o acceder a recursos altamente confidenciales, el modelo SVM de una clase detecta esta acción como una anomalía y genera una alarma.

Exposición de API no Seguras

Para abordar la amenaza de la exposición de API no seguras en entornos de redes definidas por software (SDN), se podrían usar Bosques de Aislamiento (Isolation Forests) porque pueden detectar patrones raros y sospechosos en grandes conjuntos de datos.

Los bosques de aislamiento destacan por su eficacia a la hora de detectar anomalías e intrusiones en datos no estructurados o complejos. Están diseñados para aislar eficazmente observaciones anómalas, lo que los convierte en una opción sólida para combatir la amenaza de las API expuestas en las redes SDN.

El procedimiento para detectar esta amenaza utilizando este algoritmo es recopilar información de las interacciones API de la red SDN, incluidas solicitudes, respuestas y patrones de acceso. Esta información se utiliza para crear un conjunto de datos que representa el comportamiento normal de la API.

Luego, el modelo se entrena utilizando este conjunto de datos, etiquetado como "normal". El modelo aprende a reconocer patrones típicos de interacción API en un entorno SDN. Una vez entrenado el modelo, se utiliza para realizar un seguimiento de las interacciones API en tiempo real. Si detecta un patrón de interacción que es significativamente diferente del comportamiento normal aprendido durante el entrenamiento, se activa una alarma. Esta advertencia indica que se ha detectado una exposición de API potencialmente peligrosa, lo que permite a los administradores de red tomar medidas proactivas.

Por ejemplo, si un atacante intenta realizar solicitudes no autorizadas o inusuales a través de la API de un controlador SDN, el modelo Isolation Forests puede detectar este comportamiento como una anomalía y generar una alarma. Los administradores pueden aceptar esta advertencia y tomar medidas como denegar el acceso o monitorear actividades sospechosas.

Su implementación mejora la ciberseguridad al detectar patrones de comunicación inusuales o no autorizados y permite una respuesta eficaz a esta amenaza en constante evolución en las redes SDN.

Ataques de Reconocimiento

En la contienda contra los ataques de reconocimiento en los entornos de redes definidas por software (SDN), la elección más adecuada recae en la utilización de las Máquinas de Vectores de Soporte (SVM). Estos algoritmos tienen como propósito hallar un hiperplano óptimo que permita una clasificación precisa de los datos en múltiples categorías, maximizando así la distancia entre los puntos de datos de distintas clases y minimizando los errores de clasificación.

El proceso para identificar ataques de reconocimiento implica inicialmente la recopilación de información acerca de la actividad en la red, incluyendo registros de eventos,

flujos de tráfico y solicitudes emitidas por dispositivos y controladores en la red SDN. Posteriormente, se ejecuta un procedimiento de preprocesamiento de datos con el objetivo de limpiar y estructurar la información obtenida. A continuación, se identifican características relevantes en los datos que puedan indicar actividad de espionaje, tales como escaneos de puertos o solicitudes inusuales.

En el supuesto de que el modelo SVM detecte una actividad considerablemente anormal, se genera una alerta. Esta notificación sirve como señal para que los administradores tomen medidas inmediatas con el propósito de prevenir un ataque más extenso, pudiendo incluir la restricción del acceso al dispositivo sospechoso o el bloqueo del tráfico relacionado.

Estos resultados son más que simples hallazgos; representan pilares estratégicos en la defensa contra una variedad de amenazas que pueden afectar la integridad de las redes SDN. Los Bosques Aislados se destacan por su capacidad probada para detectar anomalías, identificar patrones desconocidos y proporcionar una alerta temprana ante posibles amenazas. Por otro lado, las CNN demuestran su excelencia en el análisis de flujos de datos de tráfico de red en SDN, asegurando la detección de ataques de reenvío malicioso. Las SVM, por su parte, se erigen como guardianes contra la suplantación de identidad, mientras que los Bosques de Aislamiento juegan un papel crucial en la detección de la exposición de API no seguras en estos entornos.

A medida que avanzamos hacia un mundo cada vez más interconectado y dependiente de la tecnología, la implementación de estas soluciones se convierte en un componente esencial para garantizar la seguridad y la confiabilidad de nuestras infraestructuras de comunicación críticas. Por lo tanto, es recomendable que las organizaciones y expertos en ciberseguridad consideren

seriamente la adopción de estos algoritmos y enfoques en sus estrategias de defensa cibernética en entornos SDN.

Discusión de resultado

.

A lo largo de esta investigación, se han evaluado varios algoritmos de aprendizaje automático en términos de su efectividad para detectar y combatir diversas amenazas que pueden afectar a un entorno SDN. Entre estos algoritmos, se ha identificado que el Bosque Aislado (Isolation Forest) emerge como una elección altamente adecuada para detectar y responder a ataques dirigidos a controladores SDN. Su elección se basa en una serie de razones clave.

En primer lugar, los Bosques Aislados son altamente eficientes en la detección de anomalías. En un entorno de SDN, es esencial poder identificar actividades inusuales que podrían indicar intrusiones o ataques. Los Bosques Aislados tienen la capacidad de aislar de manera efectiva observaciones anómalas, lo que los convierte en una herramienta poderosa para detectar actividades sospechosas que pueden pasar desapercibidas mediante otros enfoques.

Otro punto relevante es la capacidad de los Bosques Aislados para detectar patrones desconocidos. A diferencia de algunos otros algoritmos que dependen de identificadores específicos de ataques previos, los Bosques Aislados no requieren conocimiento previo de amenazas conocidas. Esto significa que pueden identificar patrones de ataque que son completamente nuevos y adaptarse a amenazas emergentes. Esta flexibilidad es esencial en un entorno de SDN en constante evolución, donde los ataques pueden ser innovadores y únicos.

Otro factor crucial es la detección temprana que ofrecen los Bosques Aislados. Son capaces de identificar anomalías en una fase inicial, lo que resulta fundamental para la seguridad en SDN, debido a que permite tomar medidas preventivas antes de que los ataques causen daños graves, lo que contribuye en gran medida a proteger de manera efectiva una red SDN.

Además de los Bosques Aislados, también se ha analizado el uso de redes neuronales convolucionales (CNN) para la detección de ataques de reenvío malicioso en redes SDN, máquinas de vectores de soporte (SVM) para abordar la suplantación de identidad, y nuevamente, los Bosques Aislados para combatir el tráfico malicioso y los ataques de reconocimiento. Cada uno de estos enfoques se adapta específicamente a las amenazas particulares que pueden surgir en un entorno SDN.

Es necesario resaltar que, aunque los Bosques Aislados son poderosos en la detección de intrusiones, ningún algoritmo es infalible. Existen situaciones excepcionales en las que intrusiones altamente sofisticadas o cambios extremadamente sutiles en el tráfico de red pueden dificultar su detección. Estas circunstancias excepcionales pueden influir en la efectividad del algoritmo, aunque sigue siendo alto en la mayoría de los escenarios.

Por último, la factibilidad también puede depender en gran medida del conjunto de datos utilizado para entrenar el modelo de Bosque Aislado y de la configuración específica de la implementación. Un conjunto de datos de entrenamiento representativo y de alta calidad es fundamental para maximizar su efectividad.

Esta investigación busca proporcionar una comprensión más profunda de cómo la inteligencia artificial puede fortalecer la seguridad en las redes definidas por software, permitiendo una detección más rápida y eficaz de las amenazas, y brindando la capacidad de adaptarse a nuevos desafíos cibernéticos en constante evolución. A medida que avanzamos hacia

un futuro cada vez más conectado y dependiente de la tecnología, la integración de la IA en la ciberseguridad de SDN se presenta como un componente crítico para garantizar la continuidad y la confiabilidad de nuestras infraestructuras de comunicación.

Conclusiones

Se puede concluir que las amenazas y vulnerabilidades en las redes definidas por software (SDN) son problemas serios que debemos atender de manera activa para mantener seguras y confiables nuestras redes. Algunos de estos problemas incluyen ataques al controlador SDN y flujos maliciosos, que están relacionados con la centralización del control en SDN. La seguridad en las redes SDN siempre está cambiando así que debemos estar preparados para enfrentar nuevas amenazas y seguir consejos para proteger nuestras redes SDN.

Los algoritmos de aprendizaje automático son recursos útiles que se pueden usar para mejorar las redes definidas por software (SDN). Ayudarían hacer que estas redes sean más seguras, escalables y eficientes. Estos algoritmos pueden encargarse de tareas como dirigir el tráfico, asignar funciones y detectar anomalías. Esto hace que la gestión de las redes SDN sea más efectiva y adaptable. Al evaluar diversos algoritmos de aprendizaje automático, se puede determinar cuáles son los más adecuados para situaciones específicas.

Al identificar la eficacia de los algoritmos de aprendizaje automático en la detección de intrusiones en entornos de redes definidas por software (SDN) se destaca los Bosques Aislados (Isolation Forests) como una elección sobresaliente, debido a su capacidad demostrada para

detectar anomalías, identificar patrones desconocidos, y ofrecer una detección temprana de amenazas, elementos cruciales en la protección de las redes SDN. Los resultados obtenidos en esta investigación respaldan enfáticamente el valor insustituible y el inmenso potencial de la inteligencia artificial en el ámbito de la ciberseguridad aplicada a las redes definidas por software (SDN). Estos hallazgos no solo subrayan la relevancia de la IA en la protección de las infraestructuras de comunicación críticas, sino que también sientan una sólida base para futuras indagaciones y aplicaciones destinadas a salvaguardar la integridad de nuestros sistemas de comunicación esenciales.

Recomendaciones

Dada la constante evolución de las amenazas y vulnerabilidades en las redes definidas por software (SDN), es esencial abordar estos riesgos de manera proactiva. Se recomienda que las empresas tomen precauciones fuertes y sigan consejos buenos para proteger sus redes SDN. Esto implica actualizar SDN a menudo, usar sistemas de detección que aprenden solos y enseñar al equipo de trabajo sobre seguridad cibernética de manera constante.

Se sugiere explorar y evaluar los distintos algoritmos disponibles para encontrar los más adecuados para necesidades específicas. Una vez identificados, se pueden implementar de manera efectiva para optimizar tareas de gestión de red, como el enrutamiento y la detección de problemas. Esto permitirá una administración más flexible y eficiente de las redes SDN.

La implementación de los Bosques Aislados se recomienda como una medida esencial para fortalecer la seguridad en las redes definidas por software. Estos algoritmos han demostrado su eficacia en la detección de amenazas y la identificación de patrones anómalos, lo que proporciona una capa adicional de protección en entornos SDN. Asimismo, es fundamental mantener un enfoque continuo en la investigación y desarrollo de soluciones basadas en inteligencia artificial, adaptándolas a medida que evolucionan las amenazas cibernéticas. Esta

combinación de medidas prácticas y una mentalidad de mejora constante contribuirá significativamente a salvaguardar la integridad de las redes SDN en un entorno digital en constante cambio.

Bibliografía

Alava, C., & Paladines, D. (2020). *Dspace UPS*. Recuperado el 27 de Agosto de 2023, de https://dspace.ups.edu.ec/handle/123456789/19460

Arana, C. (Junio de 2021). Redes neuronales recurrentes: Análisis de los modelos especializados en datos secuenciales. *Econstor*. Recuperado el 10 de Septiembre de 2023, de https://www.econstor.eu/bitstream/10419/238422/1/797.pdf

Becci, G., Morandi, M., & Marrone, L. (Octubre de 2020). Diseño de sistemas de detección de intrusión en redes definidas por software: revisión basada en machine learning. *Sociedad Argentina de Informática e Investigación Operativa*, 14-31. Recuperado el 26 de Agosto de 2023, de http://sedici.unlp.edu.ar/handle/10915/121984

Becci, G., Morandi, M., & Marrone, L. A. (2019). Seguridad en la virtualización de redes definidas por software: revisión por dimensión a virtualizar. *Sociedad Argentina de Informática (SADIO)*, 1-14. Recuperado el 27 de Agosto de 2023, de http://sedici.unlp.edu.ar/handle/10915/88673

Bone, M., Rodríguez, J., Sosa, S., & Núñez, L. (2021). Aplicaciones de SDN en infraestructura de redes educativas. *Revista Indexada, Ciencia Digital, Vol. 5*(Num. 1), 219-231. Recuperado el 1 de Septiembre de 2023, de https://www.cienciadigital.org/revistacienciadigital2/index.php/CienciaDigital/article/view/1539/3893

Cobos, Y. (2021). *Universidad Politécnica Salesiana Ecuador*. Recuperado el 27 de Agosto de 2023, de https://dspace.ups.edu.ec/handle/123456789/21982

Dairon, R. (1 de Junio de 2020). *Repositorio Unimilitar*. Recuperado el 1 de Septiembre de 2023, de https://repository.unimilitar.edu.co/handle/10654/41314

Fortune Business Insights. (2 de 12 de 2022). Obtenido de The global machine learning (ML) market is expected to grow from $21.17 billion in 2022 to $209.91 billion by 2029: https://www.fortunebusinessinsights.com/machine-learning-market-102226

Guzmán, A. (13 de Junio de 2022). *Repositorio UTN*. Recuperado el 21 de Agosto de 2023, de http://repositorio.utn.edu.ec/bitstream/123456789/12561/2/04%20RED%20293%20TRABAJO%20DE%20GRADO.pdf

Incio, F., Capuñay, D., Estela, R., Valles, M., Vergara, S., & Elera, D. (2022). Inteligencia artificial en educación: una revisión de la literatura enrevistas científicasinternacionales. *Revista de Investigación de Investigación*, 353-372. Recuperado el 2 de Agosto de 2023, de https://apuntesuniversitarios.upeu.edu.pe/index.php/revapuntes/article/view/974/866

Jurado, A. (26 de Noviembre de 2018). *Word Press*. Recuperado el 2 de Julio de 2022, de https://das6sa3.wordpress.com/2016/11/26/el-sistema-educativo-grupo-2/#:~:text=Caracter%C3%ADsticas%20del%20Sistema%20Educativo%20Ecuatoriano%20y%20su%20estructura.,-Publicado%20el%20noviembre&text=CARACTER%C3%8DSTICAS%20DEL%20SISTEMA%20EDUCATIVO%20ECUATO

Lima., M., & Gavin, M. (Junio de 2019). *Kids Health*. Recuperado el 3 de Julio de 2022, de https://kidshealth.org/es/parents/fitness-6-

12.html#:~:text=Los%20ni%C3%B1os%20de%206%20a,para%20los%20ni%C3%B1os%20m%C3%A1s%20peque%C3%B1os.

Luz, A. (2022). *Repositorio Unal.* Recuperado el 25 de Agosto de 2023, de https://repositorio.unal.edu.co/bitstream/handle/unal/83450/24625353.2022.pdf?sequence=2&isAllowed=y

Manrique, R. (2 de Julio de 2021). *pontificia universidad católica del perú repositorio.* Recuperado el 27 de Agosto de 2023, de https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/19789/MANRIQUE_HUAMANI_RENZO_ESTUDIO_RENDIMIENTO_SISTEMAS.pdf?sequence=1&isAllowed=y

Mejía, J., Gonzales, M., Fernández, A., & Crespo, N. (2022). Seguridad contra ataques DDoS en los entornos SDN con Inteligencia Artificial. *Revistas UTB, Vol. 7*(Num. 3), 105-127. Recuperado el 1 de Septiembre de 2023, de https://revistas.utb.edu.ec/index.php/magazine/article/view/2844/2332

Mejía, J., Legarda, A., Agudelo, F., & Rebollar, A. (Octubre de 2021). Modelo Para Asignar Recursos Computacionales en Infraestructuras de Redes Virtualizadas Usando Mecanismos de Aprendizaje Automático. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 72-87. Recuperado el 10 de Septiembre de 2023, de https://www.proquest.com/openview/436c4790cb1ca8a43fc2246edaf45c68/1?pq-origsite=gscholar&cbl=1006393

Moreno, R. (2019). La llegada de la inteligencia artificial a la educación. *Revista de Investigación en Tecnologías de la Información, Vol. 7*(Num. 4), 260-270. Recuperado el 12 de Agosto de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=7242777

Nicolalde, W. (10 de Febrero de 2021). *Repositorio UTN*. Recuperado el 2 de Septiembre de 2023, de http://repositorio.utn.edu.ec/bitstream/123456789/10907/2/04%20RED%20254%20TRABAJO%20GRADO.pdf

Oviedo, B., Zhuma, E., Bowen, G., & Patiño, B. (2021). Voz IP seguras implementadas en redes definidas por software. *Revista de ciencias sociales, Vol. 27*(Num. 3), 111-127. Recuperado el 2 de Septiembre de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=8081760

Rendón, S. (7 de Mayo de 2020). Enrutamiento de paquetes en Redes Definidas por Software mediante Aprendizaje Automático. *Colegio de Ciencias e Ingeniería*, 2-46. Recuperado el 11 de Septiembre de 2023, de https://repositorio.usfq.edu.ec/bitstream/23000/8790/1/146125.pdf

Ruipérez, J. (2021). Seguridad en Redes definidas por software (SDN). *Universidad Politécnica De Valencia*. Recuperado el 2 de Septiembre de 2023, de https://riunet.upv.es/handle/10251/165154

ANEXOS

Figura 1

Certificado de Análisis de plagio