UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

Departamento de Ciencias de la Computación

Lectura y Escritura de Textos Académicos

Tema:

Planteamiento del Problema

Autor:

Moisés Benalcázar
Mateo Medranda
Bryan Quispe

NRC: 29765

Ecuador 2025-10-19

Tema propuesto:

Detección de Ciberataques según datos del tráfico de red

Identificación Problema:

En las redes corporativas, los atacantes suelen realizar escaneos para identificar puertos abiertos y vulnerabilidades antes de lanzar un ataque, pero es muy difícil detectar estos patrones cuando ocurren. Esto genera un problema: La baja capacidad de detección de ciberataques según información del tráfico de red.

Planteamiento Del Problema:

La ocurrencia de ciberataques a diferentes organizaciones aumenta cada año con la evolución de la tecnología, pero aún existe la dificultad frente a la detección de estos, lo cual deja una brecha de seguridad en cualquier organización que cuente con una infraestructura de red. Según GMS Seguridad, para el año 2023 hubo un aumento del 63% de ciberataques en comparación con el año 2022, y pese a la existencia de algunos métodos de detección, no se ha desarrollado un modelo inteligente para predecir la probabilidad de un ciberataque y categorizarlo mejorando la capacidad de detección y la capacidad de afrontar un tipo específico de ataque.

Objetivo de la Investigación

Desarrollar un modelo predictivo que permita anticipar ciberataques

Objetivos Específicos

- Identificar los patrones en el tráfico de red que permitan la detección de un ciberataque.
- Usar técnicas de machine learning para detección de ciberataques.
- Implementar un modelo de clasificación para detectar ciberataques.
- Utilizar métricas de evaluación para medir el rendimiento del modelo implementado.

Preguntas de investigación

- RQ1: ¿Cuáles son los patrones más comunes en el tráfico de red cuando sufren un ciber ataque?

  En el documento 3 se observa que los patrones que presentaron mayor significancia al obtener los resultados fueron: Servicio, duración, origen_bytes, origen_local, respuesta_local, historial, padres_del_túnel, etiqueta-detallada.

- RQ2: ¿Que técnicas de machine learning se aplican a la detección de patrones en tráfico de red?

- RQ3: ¿Qué métricas se pueden utilizar para evaluar el desempeño adecuado de un modelo de detección de ciberataques?

  Silhouette Score: Evalúa la separación que hay entre muestras de diferentes clústeres.

  Calinski-Harabasz Score: mide la densidad y la separación de los clústeres.

  Davies-Bouldin Score: Mide cuanto se separan los clústeres o, por el contrario, cuánto se solapan.

  Adjusted Rand Index (ARI)*:* Mide la similitud entre las etiquetas predichas por el clustering y las etiquetas reales.

  Homogeneity Score: Evalúa si cada clúster contiene solo muestras de una única clase

Métrica	Sin 'name'	Con 'name'	Diferencia
Métricas sin etiquetas reales			
Silhouette Score	0,9479	0,9293	+0,0186
Calinski-Harabasz Score	3273,11	2928,81	+344,30
Davies-Bouldin Score	0,6152	0,6294	-0,0142
Métricas con etiquetas reales			
Adjusted Rand Index	-0,0023	-0,0023	0,0000
Homogeneity Score	0,0027	0,0027	0,0000
Completeness Score	0,0773	0,0773	0,0000

Tabla 4.1: Comparativa de Métricas de Agrupamiento, *Silhouette Score*, *Calinski-Harabasz Score*, *Davies-Bouldin Score*, *Adjusted Rand Index*, *Homogeneity Score*, *Completeness Score*, con y sin la variable correlada 'name' para la base de datos Android-IoT.

- RQ4: ¿Que tecnicas se aplicaron para resolver el problema?

  En el documento 3 se indica que la metodología utilizada para resolver el problema fue de validación experimental y la ejecución se realizó mediante el método informático ciclo en V.

¿Qué es un objetivo general?

Es la meta principal que se plantea para solucionar el problema identificado en relación con el tema de investigación.

¿Qué es un Objetivo específico?

Detalla mediante metas cortas el paso a paso para alcanzar el objetivo general, dividiendo el propósito general en partes más manejables.

¿Para qué le sirven las preguntas de investigación?

Las preguntas de investigación nos ayudan a orientar y enfocar el estudio para ver lo que necesitaremos investigar, realizar y explicar a lo largo del articulo