

Clasificación de ciberataques mediante un modelo de ensemble learning

Andrés Caro Lindo
Universidad de Extremadura

Facultad de Informática
Sala de Grados - Lunes 8 de mayo de 2023 - 18:00
Entrada libre hasta completar el aforo

Resumen:

Los sistemas TI usan algoritmos de inteligencia artificial (IA) para procesar datos. La IA se utiliza generalmente para extraer conocimiento de información almacenada y, dependiendo de la naturaleza de los datos, puede ser necesario aplicar diferentes algoritmos. En esta conferencia se presenta el uso de IA orientada a ciberseguridad a través del estudio del tráfico de red. Se presentará la construcción de un modelo de clasificación de ciberataques en dos etapas, que permite separar el tráfico legítimo e ilegítimo (fase 1) al mismo tiempo que identifica el tipo de tráfico ilegítimo (fase 2). De esta forma, el sistema permite una completa clasificación multiclase del tráfico de red. La estimación del rendimiento global se realiza utilizando un conjunto de datos evaluado mediante dos enfoques. Se mostrarán los resultados del modelo desarrollado, que alcanza un F1 de 0.912 para la detección de ciberataques (fase 1) y 0,7754 para la clasificación de los ciberataques (fase 2).

Sobre Andrés Caro Lindo:

Andrés Caro, Doctor e Ingeniero en Informática, es Profesor Titular de Universidad en el Departamento de Ingeniería de Sistemas Informáticos y Telemáticos de la Universidad de Extremadura (área de Lenguajes y Sistemas Informáticos). Es el Investigador Principal del Grupo de Ingeniería de Medios (GIM) de la UEx. Desde el año 2000 imparte docencia en asignaturas de programación de bases de datos, calidad de procesos y de productos software, auditoría y legislación informática, protección de datos, análisis forense y peritaje informático, hacking ético, etc. Ha sido Director de 5 ediciones del Curso de Experto Profesional "Derecho Tecnológico e Informática Forense", y del MOOC "Investigación en Informática Forense y Ciberderecho" ofertado en Miriada_X. Es Investigador Principal en proyectos europeos y regionales, y autor de diversos artículos, ponencias e informes periciales, fue premiado en 2019 en las Jornadas Nacionales de Investigación en Ciberseguridad por el Instituto Nacional de Ciberseguridad (INCIBE) por uno de sus trabajos.