Técnicas de machine Learning para la detección de Ransomware: Revisión sistemática de literatura

Olmedo Zambrano Elkin Isaac

19 de octubre de 2023

Resumen

La presente investigación tuvo el propósito de identificar las técnicas y/o algoritmos de Machine Learning (ML) utilizadas para la detección y clasificación de las diferentes familias ransomware, así como las herramientas de software que se utilizan para la aplicación de estos algoritmos. Está revisión sistemática de literatura (RSL) se apoyó en la metodología propuesta por Bárbara Kitchenham y en el uso de la herramienta Parsifal

1. Introducción

El objetivo principal de la presente investigación fue identificar los algoritmos del Machine Learning para la detección y clasificación de las diferentes familias ransomware, así como las herramientas de software a utilizar para el entrenamiento del conjunto de datos con las cuales se puede identificar patrones, logrando así, brindar un apoyo en la detección de ransomware y de esta manera mitigar daños irreparables a la integridad de la información (Almousa M., 2021), A continuación, se detalla el desarrollo de la presente investigación, el cual se realizó en las siguientes secciones: Metodología donde se describen las fases que propone Barbara Kitchenham, posteriormente en la sección de Resultados, se analiza la información extraída de los artículos seleccionados, (Alrawashdeh K., 2018)luego se explica e interpreta de forma más específica la información en la sección de Discusión y finalmente, se especifica las Conclusiones obtenidas al elaborar la RSL. (?, ?).

2. DISCUSIÓN Y RESULTADOS

A continuación, se detallan cada una de las tareas realizadas durante la etapa de planificación de a revisión sistemática de literatura:

- Planificar la revisión sistemática de literatura.

- Establecer el proceso de búsqueda: Se definen las palabras claves.
- Establecer el proceso de búsqueda: Se describe el criterio a seguir para la selección de estudios.
- Cadenas de búsqueda
- Verificación de calidad

A continuación se describen los pasos para desarrollar la revisión sistemática de literatura.

- Busqueda de artículos
- Evaluación de calidad a los artículos primarios
- Extracción de la información

2.1. Análisis y clasificación de la información

Análisis de algoritmos: Se tomó en cuenta el número total de artículos donde se menciona los algoritmos utilizados, estos datos se los representó en un grado porcentual para hacer visible de una mejor manera la información en la Figura 1.

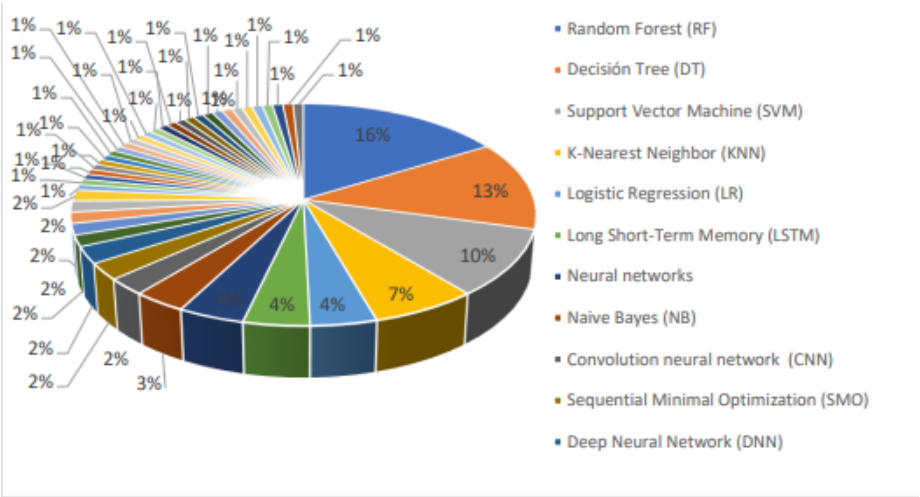

Figura 1: Algoritmos utilizados

Al observar y analizar la Figura 1 se puede determinar lo siguiente:

- El algoritmo Random Forest (RF) con el 16 porciento obtiene un porcentaje mayor en el gráfico, debido a que engloba a varios artículos donde se utiliza este algoritmo comotécnica del machine learning para la detección de ransomware.

- Decisión Tree (DT) obtiene el 13 porciento de usabilidad; Máquina de Vectores de Soporte (SVM) es usado en el 10 porciento de los artículos; El algoritmo K-Nearest Neighbor (KNN) es utilizado en el 7 porciento de los artículos analizados.

Análisis de herramientas: Se tomó en cuenta el número total de artículos donde se menciona los métodos de extracción, estos datos se los represento en un grado porcentual para hacer visible de una mejor manera la información en la Figura 2.

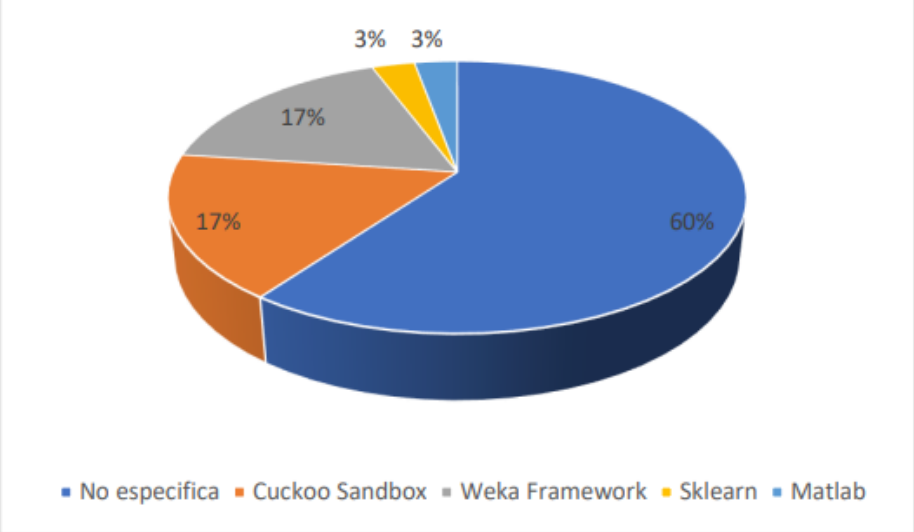

Figura 2: Herramientas utilizadas

2.2. Informe del Mapeo Sistematico En el siguiete aparatado se dan a conocer las respuestas de las preguntas de mapeo sistemático, que se realizaron con anterioridad.

2.3. Análisis de la revisión sistemática En el siguiete aparatado se dan a conocer las respuestas de las preguntas de la revisión sistemática, que se realizaron con anterioridad.

3. DISCUSIÓN

En este apartado obtenemos como la extracción de la información facilitó responder las preguntas de mapeo.s. Además, se determinó cuales son los autores más relevantes que aportan activamente en investigaciones para la detección de ransomware a través del uso de técnicas del machine learning. Después se procedió a dar contestación a las preguntas de la revisión.

.

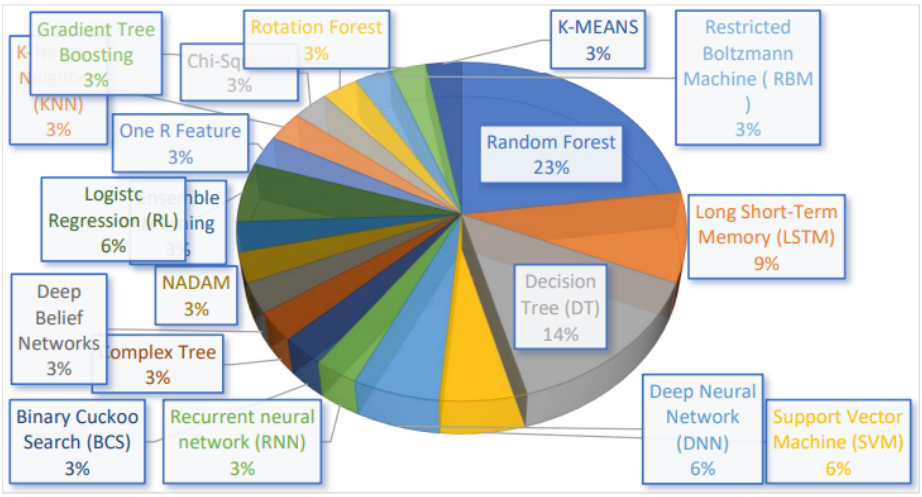

Figura 3: Principales Técnicas y/o algoritmos encontrados

4. Conclusiones

Finalmente el uso de las herramientas de Parsifal permite optimizar y desarrollar eficazmente los procesos productivos. Una revisión de la literatura sobre sistemas de planificación que contribuyen a la investigación en gestión. Realizar metódicamente una serie de extracciones precisas y específicas. Información sobre artículos relevantes que cumplen con los criterios de inclusión y Definir excepciones para identificar técnicas de aprendizaje automático. Detección de ransomware. Entre los 34 artículos analizados se encontraron los métodos más utilizados. La detección de ransomware incluye: Algoritmo de bosque aleatorio (RF) mencionado en la mayor parte de la literatura. Artículos seleccionados como los mejores en detección y clasificación Ransomware seguido de árboles de decisión (DT) y memoria larga a corto plazo (LSTM).

Referencias

Almousa M., O. J. y. A. M. (2021). Identification of ransomware families by analyzing network traffic using machine learning techniques. *Neural Networks: Tricks of the Trade*, 19–24. doi: 10.1109/TransAI51903.2021.00012

Alrawashdeh K., y. P. C. (2018). Ransomware detection using limited precision deep learning structure in fpga. *En NAECON 2018 - IEEE National Aerospace and Electronics Conference*, 152–157).