

Informe del Código del Trabajo Extracalse

CLASIFICACIÓN DE SITIOS WEB DE PHISHING

AUTORES:

Carlos Brayan Rámila Chorens

Alejandro Santana Viamontes

Alejandro Labaut Caro

Javier González Jiménez

Kevin Peña Pérez

Introducción

El presente trabajo tiene como objetivo desarrollar un modelo de clasificación para identificar sitios web de phishing utilizando el *dataset Phishing Websites* (Mohammad & McCluskey, 2015). El equipo de desarrollo esta formado por cinco estudiantes del grupo 4402 de la Facultad de Tecnologías Interactivas.

A continuación, se detallan los participantes en la solución con sus responsabilidades:

1. Carlos Brayan Rámila Chorens: Implementar la visualización de los resultados del modelo entrenado.
2. Alejandro Santana Viamontes: Realizar el entrenamiento del modelo.
3. Alejandro Labaut Caro: Realizar el entrenamiento del modelo.
4. Javier González Jiménez: Probar modelo por el reporte de clasificación.
5. Kevin Peña Pérez: Probar modelo por el reporte de clasificación.

Desarrollo

En este trabajo para el cumplimiento del objetivo se desagrega el contenido en los siguientes acápite: información general acerca del dataset empleado, explicación del proceso *Knowledge Discovery from Database* (KDD) y se finaliza con la medición del comportamiento de las clasificaciones de los diferentes métodos utilizados mediante métricas.

- **Descripción del Dataset:**

El dataset contiene 11,055 instancias y 30 atributos, todos de tipo entero {-1, 0, 1}. El atributo objetivo es 'Result', el cual indica si una URL es phishing (valor -1) o legítima (valor 1).

- **Descripción del proceso de KDD:**

El proceso de KDD consta de una secuencia iterativa de etapas, las cuales se describen a continuación según su uso:

1. Integración y recopilación: Se eligió el dataset de *Phishing Websites*.
2. Selección, limpieza y transformación (*pandas* - *Python Data Analysis Library*, s/f): Se verificó la existencia de filas duplicadas y se eliminaron. Se verificó que no hubiera valores nulos y no se requirió transformación de datos.
3. Minería de datos: Se aplicaron tres métodos de clasificación: Árbol de decisión, Perceptrón simple, *k-nearest neighbors* (KNN).
5. Evaluación e interpretación: Se usaron métricas de exactitud, precisión, recall y F1-score.

- **Métricas utilizadas:**

A continuación se detallan las métricas utilizadas (Pedregosa et al., 2011), para validar la efectividad del modelo entrenado con el dataset *Phishing Websites*.

- Métrica 1. Exactitud (*Accuracy*): Proporción de predicciones correctas .

$$\text{Exactitud} = (TP + TN) / (TP + TN + FP + FN)$$

- Métrica 2. Precisión (*Precision*): Proporción de verdaderos positivos sobre el total de predicciones positivas.

$$\text{Precisión} = TP / (TP + FP)$$

- Métrica 3. Ratio de los verdaderos positivos (*Recall*): Proporción de verdaderos positivos sobre el total de positivos reales.

$$\text{Recall} = TP / (TP + FN)$$

Conclusiones

Con la realización de este trabajo se concluye que el modelo más efectivo en la clasificación del dataset *Phishing Websites* fue Árbol de decisión, con una exactitud del 94%. Mientras que los modelos KNN y Perceptrón Simple tuvieron una exactitud del 92% y 90% respectivamente. Queda demostrado la capacidad de Árbol de decisión de manejar mejor la complejidad de los datos a partir de las métricas empleadas.

Recursos educativos usados

1. Videos educativos sobre clasificación y preprocesamiento de datos en pandas.
2. Mohammad, R., Thabtah, F., & McCluskey, L. (2012). An assessment of features related to phishing websites using an automated technique. International Conference for Internet Technology and Secured Transactions.
3. Mohammad, R., & McCluskey, L. (2015). *Phishing Websites*.
4. *pandas—Python Data Analysis Library*. (s/f). Recuperado el 1 de julio de 2024, de <https://pandas.pydata.org/>
5. Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, E. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 12, 2825–2830.