**Uniritter Campus FAPA**

Matheus Pereira Silva, Nilso José Miguel da Silva Júnior

**A3 INTELIGENCIA ARTIFICIAL**

**Phishing datasets**

**Porto Alegre, 2024**

**SUMÁRIO**

1. **INTRODUÇÃO……………………………………………………………………….3**
2. **TEMA………………………………………………………………………………….3**
3. **MÉTODO DE TRABALHO………………………………………………………….3**
4. **OBJETIVO……………………………………………………………………………3**
5. **DESCRIÇÃO DOS DATASETS……………………………………………………3**
6. **PÓS PROCESSAMENTO………………………………………………………..…4**
7. **FUNCIONALIDADES………………………………………………………………..5**
8. **RESULTADOS……………………………………………………………………….5**
9. **COMPARAÇÃO ARTIGO…………………………………………………………..7**
10. **PRINCIPAIS FATORES……………………………………………………….…….8**
11. **CONCLUSÃO…………………………………………………………….……..…10**
12. **REFERÊNCIAS……………………………………………..……………………..11**

**Introdução:**

Neste documento será apresentado o desenvolvimento de uma análise de 4 datasets voltados à busca de URLs com possibilidade de phishing em sua estrutura, o programa irá buscar por meio de classificação e irá prover a porcentagem de sua eficácia.

**Tema:**

Informar se no URL há possibilidade de phishing ou não.

**Métodos de Trabalho:**

Utilizamos o Orange como principal programa e datasets massivos encontrados de diversos sites.

**Objetivos:**

O principal objetivo deste projeto é criar um modelo de machine learning

capaz de classificar URLs como phishing ou legítimo. Usaremos métricas como

acurácia, precisão, recall e F1 score.

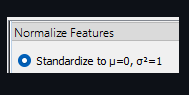
**Descrição dos Datasets:**

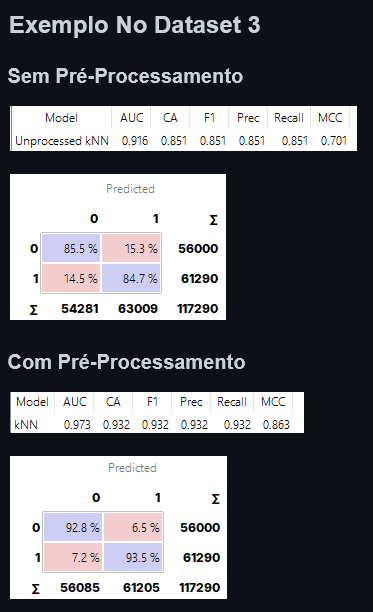
Datasets usados neste projeto contém diversos fatores como tamanho

do URL, uso de HTTPS, Domínio, endereço de IP, uso de caracteres especiais, entre outros.

**Pré-processamento:**

Foi utilizado pré-processamento apenas para o algoritmo kNN, uma vez que nenhum dos datasets contém missing data, não foi necessário remover data irrelevante ou duplicada. Para o algoritmo kNN utilizamos a métrica de normalização para garantir uniformidade no modelo, para demonstrar isso foi testado o desempenho do kNN antes e depois do pré-processamento utilizando o dataset 3.





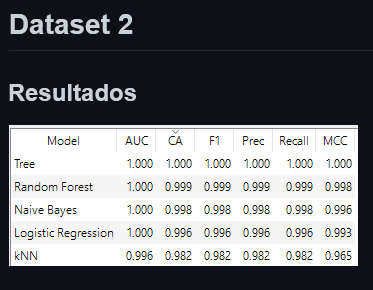
**Funcionalidade:**

Com a organização dos datasets e seus algoritmos de análise, o programa Orange, montado com pré-processamento e sem, indica dados de sua eficácia em cada algoritmo para a separação de possíveis URLs mal intencionados. Foram utilizados como método de busca o kNN, Árvore de Decisão, Naive Bayes, Random Forest e Regressão Logística. Os datasets foram divididos em datasets de treino e teste 80% e 20% respectivamente.

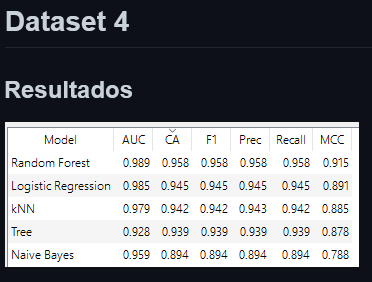
**Resultados:**

Testando os 5 algoritmos nos 4 datasets, podemos observar que, Random Forest obteve os melhores resultados, sendo o mais preciso entre os 5, logo depois temos Regressão Logística, kNN e Árvore de Decisão com resultados relativamente parecidos e sendo alternativas viáveis. Por último, temos o Naive Bayes com o pior desempenho entre os algoritmos escolhidos.



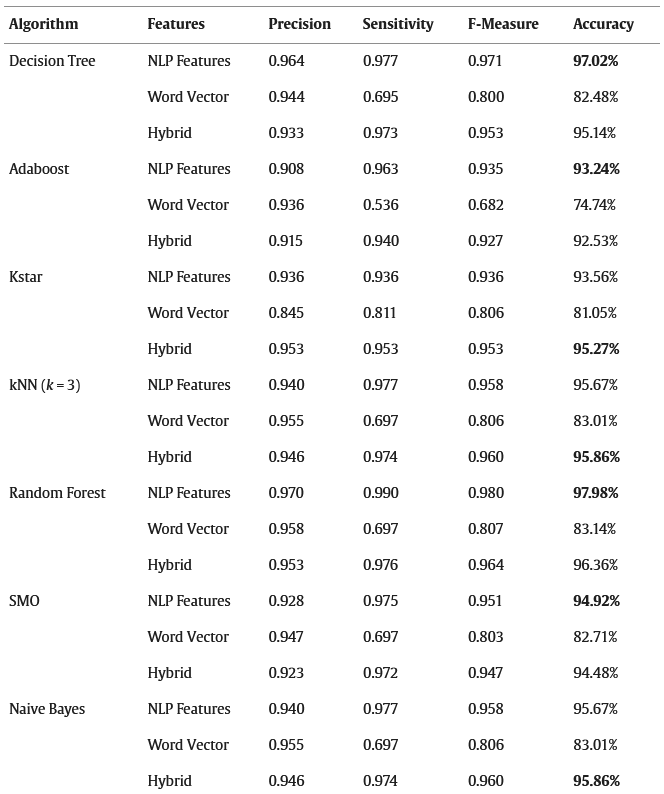






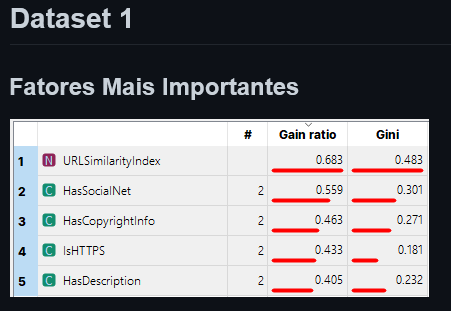
**Comparação Artigo:**

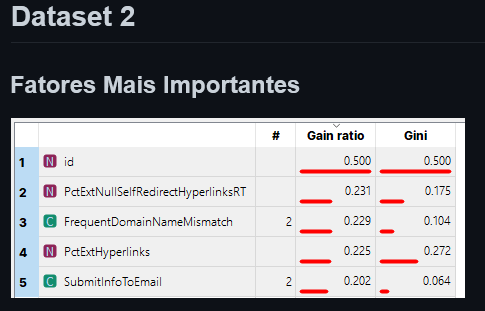
Comparando os resultados com o artigo de nossa escolha, observamos que nossos resultados foram semelhantes. No primeiro dataset nossos resultados foram mais precisos, porém, no quarto dataset os resultados foram inferiores em comparação ao artigo selecionado.

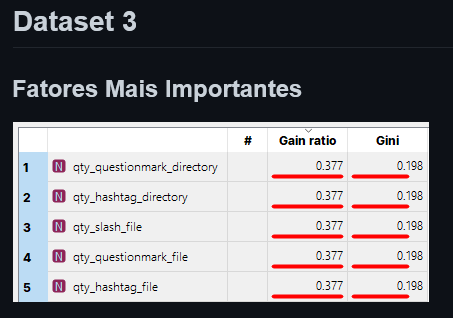


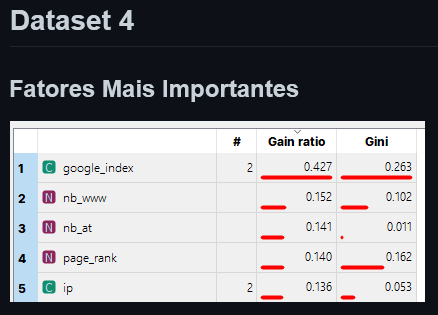
**Principais Fatores:**

Analisando os principais fatores entre os datasets podemos notar que, o uso de caracteres especiais, hyperlinks e falta de HTTPS, são fatores decisivos para determinar se determinado URL pode ser considerado phishing ou não.









**Conclusão:**

Os métodos de machine learning explorados neste documento se provaram eficientes e precisos para detectar websites de phishing. Utilizando fatores como o uso de HTTPS, nome de domínio, idade do domínio, entre vários outros. Para determinar a legitimidade de uma URL. Para aplicações futuras sugerimos um sistema para incorporar a análise da URL em tempo real, visando implementar esse sistema dentro de inboxes de e-mails e conversas em redes sociais.

**Referências**

Prasad, A., & Chandra, S. (2023). PhiUSIIL: A diverse security profile empowered phishing URL detection framework based on similarity index and incremental learning. Computers & Security, 103545. doi: <https://doi.org/10.1016/j.cose.2023.103545>

Tan, Choon Lin (2018), “Phishing Dataset for Machine Learning: Feature Evaluation”, **Mendeley Data**, V1, doi: 10.17632/h3cgnj8hft.1

G. Vrbančič, I. Jr. Fister, V. Podgorelec. Datasets for Phishing Websites Detection. Data in Brief, Vol. 33, 2020, DOI: [10.1016/j.dib.2020.106438](http://dx.doi.org/10.1016/j.dib.2020.106438)

Hannousse, Abdelhakim; Yahiouche, Salima (2021), “Web page phishing detection”, **Mendeley Data**, V3, doi: 10.17632/c2gw7fy2j4.3

VRBAN, Grega; FISTER JR, Iztok; PODGORELEC, Vili. Datasets for phishing websites detection. **ScienceDirect,** 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352340920313202>. Acesso em: 03 dez. 2024.

SALVIANO, Edgard Mesquita; SANTOS, João Pedro Ribeiro; SILVA, Matheus Almeida. Principais tipos de ataques Phishing e mecanismos de segurança. **Uniceplac,** 2021. Disponível em: <https://dspace.uniceplac.edu.br/bitstream/123456789/1611/1/Edgard%20Mesquita%20Salviano_%20Jo%C3%A3o%20Pedro%20Ribeiro%20Santos_Matheus%20Almeida%20e%20Silva.pdf>. Acesso em: 05 dez. 2024.

ALEROUD, Ahmed; ZHOU, Lina. Phishing environments, techniques, and countermeasures: A survey. **ScienceDirect,** 2017. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0167404817300810>. Acesso em: 05 dez. 2024.

SAHINGOZ, Ozgur Koray; BUBER, Ebubekir; DEMIR, Onder; DIRI, Banu. Machine learning based phishing detection from URLs. **ScienceDirect,** 2019. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0957417418306067?casa_token=wm6Tsg9Go5UAAAAA:DEVAVOKRvEcDp0NruzpwMtKO3-eaasvILcPgCGMlHGnQQkeS2SXdC5P6T8hXqG3c9Cfu9Egn55U#tbl0005>. Acesso em: 05 dez. 2024.