Nicolas Montes, Machine Learning Engineer

Montevideo, Uruguay, +598099978166, nico.montes400@gmail.com

LINKS

Web application attacks detection using deep learning (link to the article), Waf Mind Project, Eyecue Insights

---

PROFILE

I'm an Statistician with a BSc degree in Statistics (2018). In November of 2021 i finished a MSc in Machine Learning and Data Science from Facultad de Ingeniería de la Universidad de la República, Uruguay (FING-Udelar).

My main research interests focus on Machine Learning and Deep Learning, with applications in different areas like Text Processing, Computer Vision, and Network Analysis. Also, another research interest is Explainable AI (XAI).

In June 2018 i joined Eyecue Insights, a Machine Learning consultancy company and a social media analytics tool that blends big data analytics with proprietary artificial intelligence (AI) algorithms, where I currently hold a Lead Machine Learning Engineer position.

Between September of 2018 and November of 2021, I joined a research team called WAF Mind (https://www.fing.edu.uy/inco/proyectos/wafmind). At WAF Mind, I worked on applying machine learning and deep learning techniques to increase the level of assurance of web applications, which was the subject of my MSc's thesis (with a support given by ANII). The work gave rise to an article (when i was the first author) that was accepted in the 25-th Iberoamerican Congress on Pattern Recognition called: Web application attacks detection using deep learning. The paper was nominated for the best paper award.

EMPLOYMENT HISTORY

Sep 2018 — Aug 2023

Senior Researcher, Waf Mind
Montevideo

At WAF Mind, I worked on applying machine learning and deep learning techniques to increase the level of assurance of web applications. To be more specific, I worked in investigating the use of deep learning techniques to improve the performance of web application firewalls (WAFs), systems that are used to detect and prevent attacks to web applications. We model the problem as a one-class supervised case and build a feature extractor using deep learning techniques. We treat the HTTP requests as text and train a deep language model with a transformer encoder architecture (RoBERTa) which is a self-attention-based neural network.

The use of pre-trained language models has yielded significant improvements on a diverse set of NLP tasks because they are capable of doing transfer learning. We use the pre-trained model as a feature extractor to map an HTTP request into a feature vector. These vectors are then used to train a one-class classifier. We also use a performance metric to automatically define an operational point for the one-class model. The experimental results show that the proposed approach outperforms the ones of the classic rule-based Mod-Security configured with a vanilla OWASP CRS and does not require the participation of a security expert to define the features.

Jun 2018 — Aug 2023

Lead Machine Learning Engineer, Eyecue
Montevideo

Eyecue Insights is a Machine Learning consultancy company and a social media analytics tool that blends big data analytics with proprietary artificial intelligence (AI) algorithms. I am working on designing and developing machine learning and deep learning systems end-to-end. My tasks consist to find an effective feature road-map, running and evaluating different models and deploy it into production.

I leaded several machine learning projects, below i listed some of them (and detailed at a high level):

- Name Entity Recognition (NER) training and deploying into production.
- Unsupervised keyword Extraction using a Zero Shoot Classifier and the SHAP values.
- Find similar words to a target dictionary using BERT embeddings and a similarity metric.
- Video Analysis, find the most important scenes and apply a image classification in the most important frames.
- Zero Shoot Classification (for text and for images).
- Image Classification, Text Classification, and fine tuning a transformer-based network using text and images embeddings together.
- Audio Classification.

EDUCATION

2012 — 2016

Bachelor's degree, Statistics, Universidad de la República, Uruguay
Montevideo

| 2019 — 2021 | Master of Science -MS, Machine Learning and Data Science, Universidad de la República | Montevideo |

SKILLS

Deep Learning	Expert	Docker	Expert
Computer Vision	Expert	Git	Expert
AI / ML / NLP	Expert	Python	Expert
Machine Learning	Expert	Pytorch	Expert

INTERNSHIPS

| Mar 2017 — Mar 2018 | Reseach Intern, ICT4V | Montevideo |

ICT4V is a Technology Center created for leveraging the opportunities of Information and Communications Technologies (ICT) as a major driver of innovation in all sectors of activity. I worked on applying Hidden Markov Models techniques to increase the level of assurance of web applications, which was the subject of my bachelor's thesis (with a support given by ICT4V).

REFERENCES

Phd. Eng, Gustavo Betarte from Waf Mind - CTO of Tilsor

gustun@fing.edu.uy · +59899670520

Phd. Eng, Alvaro Pardo from Waf Mind - Dsense Founder

apardo@ucu.edu.uy · +598099109735

Eng. Carolina Bañales from Eyecue Insights - Founder

carolina@eyecueinsights.com