UMAN

Simpler for humans. Harder for bots

PRESENTATION

Uman is **an application extension** that collects human user events (mouse clicks, typing speed, cursor movements, etc.) and compares them to computers (bots: program replicating human actions) **to enable the detection of fraud** or spam on online sales, ticketing or social networking sites.
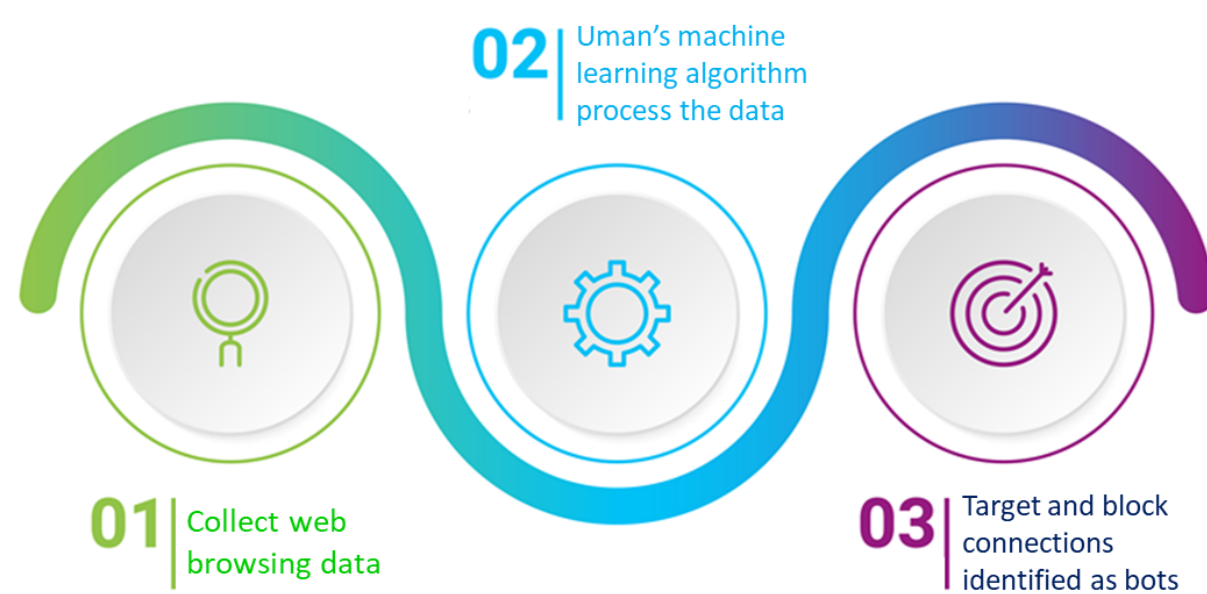
FEATURE

We simply deliver you an extension to add to your website. This extension communicates with our servers and analyzes user behavior using state-of-the-art Machine Learning models. You are warned if a robot is detected, Allowing you to block malicious behavior.

1.BLOG WEBSITES

The first step was to create our protection target : a website. We made the choice to create a Blog where users can input comments. This could be an entry point for an attacker to sent thousand of comments. The site was built using web technologies : HTML, CSS, PHP.

2.ROBOTS

To understand and train our Machine Learning model, we have created multiple fake users, acting differently on websites. To do so we used Python and Celenium library to create automation. Robots are programmed to flood comments on a website.

02 Uman's machine learning algorithm process the data

01 Collect web browsing data

03 Target and block connections identified as bots

3.MACHINE LEARNING TRAINING

Machine Learning needs data to be trained on. So we created a JavaScript Google Chrome extension in order to collect data from test users. By collecting comportments of human during servals weeks, we are able to get insight of it and find differences with robots.

4.DATA COLLECT

To make our solution simple, keep our core technologie secret and control it's usage, we have decided to build it as an API (Application programming interface). The company only install JavaScript scripts on it's website, which collect users events. An HTTP POST request is then sent to a Firebase Cloud Function, which is in charge of the detection and returns the result of the analysis

5.DETECTION

We have chosen Supervised Machine Learning in Python using fraud detection algorithms. Our goal is to make a classification of the user as fake or legit. Machine Learning is a good technology for this king of problems where we don't know exactly what a fake user's comportment can look like, but where we can teach the algorithm how real users are using a website.

OUR CLIENTS

This product is particularly aimed at companies with a website, which requires protection of user accounts or products offered for sale. It will also be useful for sites with comment sections to ensure the purity of the site.

OUR COMPETITION

reCAPTCHA

WHAT MAKES US UNIQUE ?

- We are completely transparent to provide a quality user experience

- we adapt to the different laws applicable on each of our clients' sites

Small Business

100 K Queries/month

Maintenance
Business trips
Custom legal terms

- Monthly : 2600€
- Yearly : 24K€

Corporate

1M Queries/month

Maintenance
Business trips
Custom legal terms

- Monthly: 5200€
- Yearly: 48K€

Enterprise

5M Queries/month

Maintenance
Business trips
Custom legal terms

- Monthly: 13000€
- Yearly: 120K€