Digital fingerprinting and sign-in-less profiles for the Big Data and GDPR era

Teele Annus, SecureBadger

What?

Javascript front-end library with a Node.js/Python backend to generate a website user’s digital “fingerprint” that can be decoded using machine learning methods.

For whom?

Securebadger is a startup that offers a platform for residential rental real estate portfolio management and risk assessment that allows long-term real estate investors and property owners to manage all aspects of their portfolio and utilizes machine learning models to assess the financial and behavioral risks of their tenants and the associated rental contracts.

Why?

GDPR stipulates specifically what and how personal data can be gathered and used. At the same time the business model of Securebadger requires the retention of large amounts of user-generated data to train machine learning models. The need to anonymize the personal data of rental applicants on one hand and the need for a user-friendly experience on the platform necessitate a software solution where current users can be matched with past users in the database without the use of user profiles and personal data (name, birthdate, personal code).

The solution?

A combination of highly persistent cookies, device and user fingerprinting can theoretically match past users in the database with a current user session without using user profiles and personal data. These technologies are partly used by fraud detection platforms such as Threatmetrix, but due to their different business requirements they do not utilize all of the available methods. Our solution is to combine highly persistent cookies, device data, geolocation data (to what extent it is available) and user interaction data (mouse and keyboard usage patterns on the website) with machine learning methods to match users with a sufficiently high degree of confidence.

The project outcome?

A Javascript library that runs in the frontend on the pages where the intended users fill in HTML forms and produce mouse clicks and a Node.js or Python backend that receives the session data, stores it in a NoSQL database and converts it into variables that can be further used by machine learning models. The exact data to be captured and stored during the user session and the subsequent transformations into model-usable data will be specified with the project team.

The benefits?

The intellectual property will be owned jointly by the development team and Securebadger with 40% of the rights assigned to the development team. In case of licensing the technology to third parties, the development team will be entitled to 40% of the licensing fees. There is also the possibility for the team members to join the startup under with options contract.

Main point of contact for the project will be Securebadger co-founder and CEO Teele Annus (teele.annus@securebadger.com)

Technical point of contact for the project will be Securebadger co-founder and Head of Data Science Karl Märka (karl.m2rka@gmail.com)