Software Requirements Specification Document

Written by Enna Grigor

Project:

Web based tool that identifies dangerous users in social media networks via text and images.

Overview:

1. Introduction

We will start by introducing the product –
The product is web-based tool that identifies dangerous users in social media networks via text and images.

1.1 Purpose

The purpose of the product is to scan social media platforms that have public APIs and extract text and images, then it will monitor and identify keywords according to a pre-defined "dangerous" vocabulary. With the help of both types of monitoring and identifying (text and image) we can maintain a list of suspicious people who may pose a social danger.

1.2 Intended Audience

The intended audience can be split into two categories:
The first one is security organizations.
The second one is private civilian companies.

1.3 Intended Use

The intended use for security organizations is identifying potentially dangerous users online and monitoring their activities.
The intended use for private civilian companies is to perform a background scan for a new employee in the company.

1.4 Scope

The tool will scan text and images from social networks that have public API.
The main goal is to focus on popular APIs for example Twitter, Facebook, YouTube. The text extracted can come from comments, posts, published links. During the scan the tool will monitor and identify keywords according to a pre-defined "dangerous" vocabulary.
For example words like massacre, killing spree, murder, guns, etc.
The tool will scan the images posted by users with the help of image detection, it will identify and alert on images that constitute "red lights" such as images with weapons, flags of terrorist organizations, etc.
With the help of both types of monitoring and identifying (text and image) we can maintain a list of suspicious people who may pose a social danger.
Then, the goal is to classify the level of risk of those people on the list.
For example:

- Risk classification of how "dangerous" the person is.
  (red flag, orange flag, yellow flag, green flag)
- Whether the risk is social or political (dangerous to the country).
- How many more "dangerous" friends the same user has.
- In what geographical area the user inhabits.

Another feature is the ability to enter a username/full name of a user, select criteria and search for it according to those criteria and thus check if it poses a social danger.

1.5 Risk Definitions and Acronyms

Some risks may include:

a. Defining non-dangerous users as “dangerous” based on false-positive classification.
b. Defining dangerous users as “non- dangerous” based on false-negative classification.
c. Privacy violation.

2. Overall Description

The project is a web-based tool that identifies dangerous users in social media networks via text and images.
After some research online – there are similar products that offer these services for example – the company Cobwebs that focuses on systems that service the national security, law enforcement and private sectors, identifying web relations, criminal activities and cyber terrorist threats.
Unlike Cobwebs – our product is also intended for a more general scan (so it can be used by private companies that want the HR run a background check before hiring) and not necessarily only for security-based organizations.

2.1 User Needs

Because our product can be used by two different types of users – the needs will be split into two categories:

Security organization:

❖ User friendly layout (the website should be easy to use and data should be displayed in way that could be analyzed easily).
❖ The scan should display the source – so if the person who analyzes the data displayed could go to the source and make a final verdict (if the data displayed a false/doubtful classification of the information).
❖ The data from the scan should be displayed based on the categories that are in natural order (if we are searching for a person – What will we search first?) -
First the user’s name and their risk level, then the links to the social media the user has, the geographical area, then the data that classified this user as “dangerous” – etc.
❖ The scan should run smoothly with a reasonable time.
❖ A “report false verdict” button so that the client could report false classification so that the developers could always improve the classification.

Private organizations:

- User friendly layout – Obvious place to insert the person's name in order to execute the can.
- The results should be easy to read – off the bat the user should be classified if dangerous or not (if not – the scan results will simply display – "no dangerous information found – user cleared".
- The level of risk should be displayed first (if risk is found).
- If the user is classified as dangerous – then the data that classified the user as "dangerous" should be displayed with links (to make sure that the person who scans - has the opportunity to see why the product made a verdict that user is dangerous).
- The scan should run smoothly with a reasonable time.
- A "report false verdict" button so that the client could report false classification so that the developers could always improve the classification

2.2 Assumptions and Dependencies

The dependencies this project has are:

- That amount of information the public API's of the social media's platform offer access to.
- The privacy configuration that user has – if the user is private (then we cannot access the content of their profile) – we have to assume that there is enough public information to rely on.
- A library of images of weapons (already collected by a public project on GitHub - https://github.com/ivaibhavkr/Weapon-Detection-And-Classification)

  - note: Library may be changed later in the project
- Python machine learning libraries.

3. System Features and Requirements

3.1 Functional Requirements

- The product will scan text and images from social networks that have public API.
- The text extracted will come from comments, posts, published links.
- During the scan the product will monitor and identify keywords according to a pre-defined "dangerous" vocabulary.
- With the help of both types of monitoring and identifying (text and image) the product will maintain a list of suspicious people who may pose a social danger.
- Risk classification will be classified based on how "dangerous" the person is. (red flag, orange flag, yellow flag, green flag).
- The product will display whether the risk is social or political (dangerous to the country).

- The product will display a list of other dangerous “friends” the user has (if found).
- The product will display the geographical area the user is active on.
- The product will allow the user to scan a specific name they insert in order to see if they have “dangerous” behavior.
- The information extracted will be displayed in a user-friendly way so that it could be easily analyzed (via graphs, maps, links, etc.).
- The system will allow a “false verdict” report that can be sent to the developers so it could always be improved.

3.2 Systems Requirements

The goal is that the only requirements that the user shall have are a computer and access to a stable internet connection because it is a web-based tool.

3.3 Nonfunctional Requirements

- The product will be on web-based platform.
- Only registered users can use product after login authentication.
- The client side will be written in react.
- The server side will be written in GO.
- The database that will be used to store the information will be a key-value based database.
- The website should load in 3 seconds when the number of simultaneous users is > 10000.
- When scanning a specific user – it should not take more than 5 minutes.
- When scanning the social media – for dangerous users – the scan will be executed until told otherwise.
- The product will send an error while scanning if the user has unstable internet connection or an error occurred.
- Each successful login will be recorded in an audit trail.