Functional Specification Document

By Artur Katelovic – C00242207

Introduction

In this document I will cover what my application/add-on is, what does it do and how it will work. I will also talk about its core functions which are functions that will be in the application/add-on, I also talk about some other function that won't be core function, but I would still like to have it in my add-on.

The other topics I cover in this is who will be using my add-on so the target users. In this document I have also created a Context and Use Case Diagram for my add-on. I also have the Metrics so I could have something to judge my project progress on and if I accomplished my goal with my add-on. And finally, I also have covered where I got my ideas from for my add-on, in that topic I talk about other applications that are similar to what I have to do.

What is the application supposed to be?

My application is supposed to be a web browser add-on that will scan a website using different technologies, languages, tools and libraries to check if the website that the user went to is a cloned website or a legitimate website and warn the user that the website, they are trying to access is a fraudulent website and prevent them for accessing it.

What will it do?

Core functions

- The main function of my application/add-on will be to decide whether a website is cloned or a legitimate website, so in order to achieve this I will use a Named Entity Recognition and JavaScript I will check the URL that the user tries to access and check the speeling on that website and take that data to check if its cloned or not.
- It will also have function that will allow it to get the URL and send to "virustotal" using an API to scan it for virus and then get the results and store them for another function.
- Have a points system that will decide if the website is cloned or not, so after I get the results from the scan it will compile them and give them a score and if the score is above a certain point it will mark the website as a cloned malicious website.
- Once the application decides that the website is cloned it will then block the user from accessing that website and warn them that the website they are trying to access is cloned and malicious and that it would be best to stay away from it.

Other functions

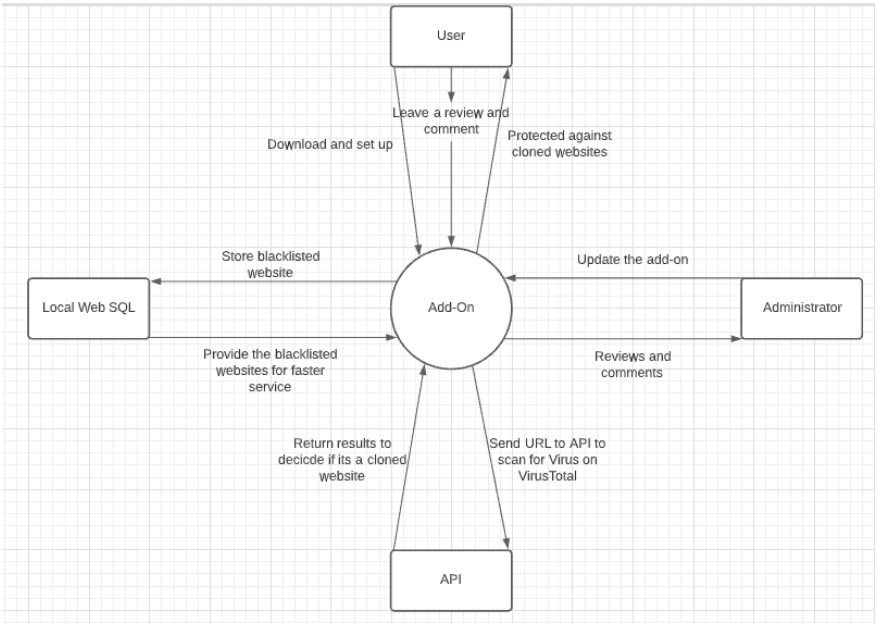
- A function that I would like to add if I have enough time is a function that will get the URL of the website that it marked as cloned/malicious and store it in the local web SQL so that in future when the user tries to access that website again it will no longer need to scan that website it will already know that it's a cloned website already, so it will make it much faster and more efficient.

Who is going to be using it?

Since my application/add-on is going to be made for chrome the user base will be anyone who uses chrome as their main browser on their laptop or desktop.

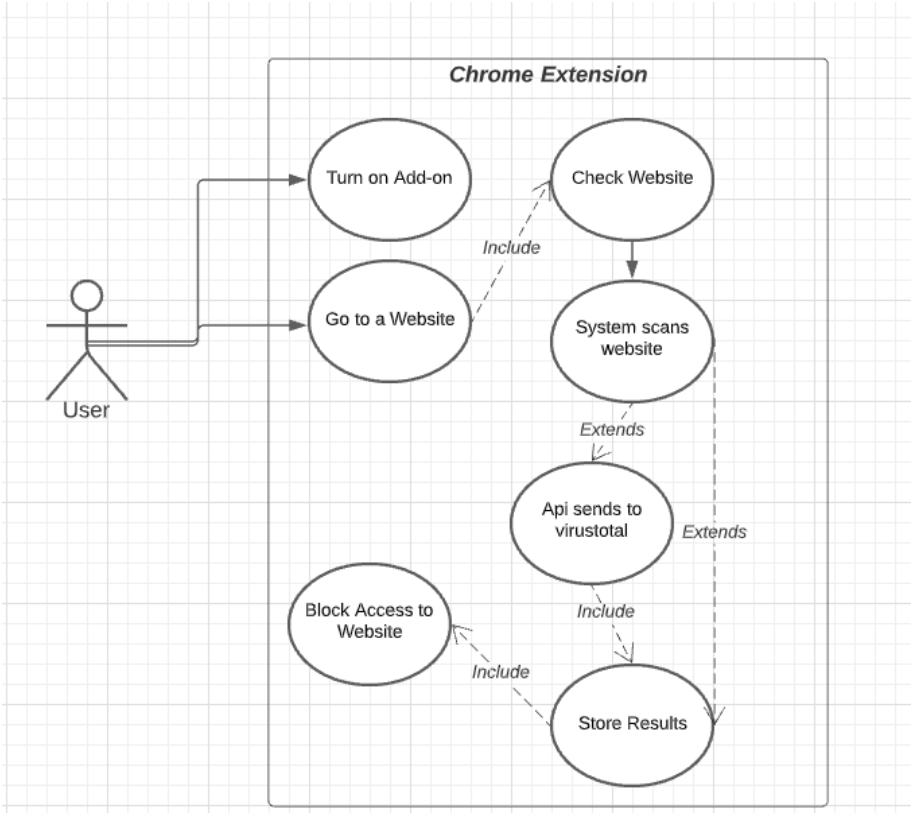
Context and use case diagrams

Context Diagram



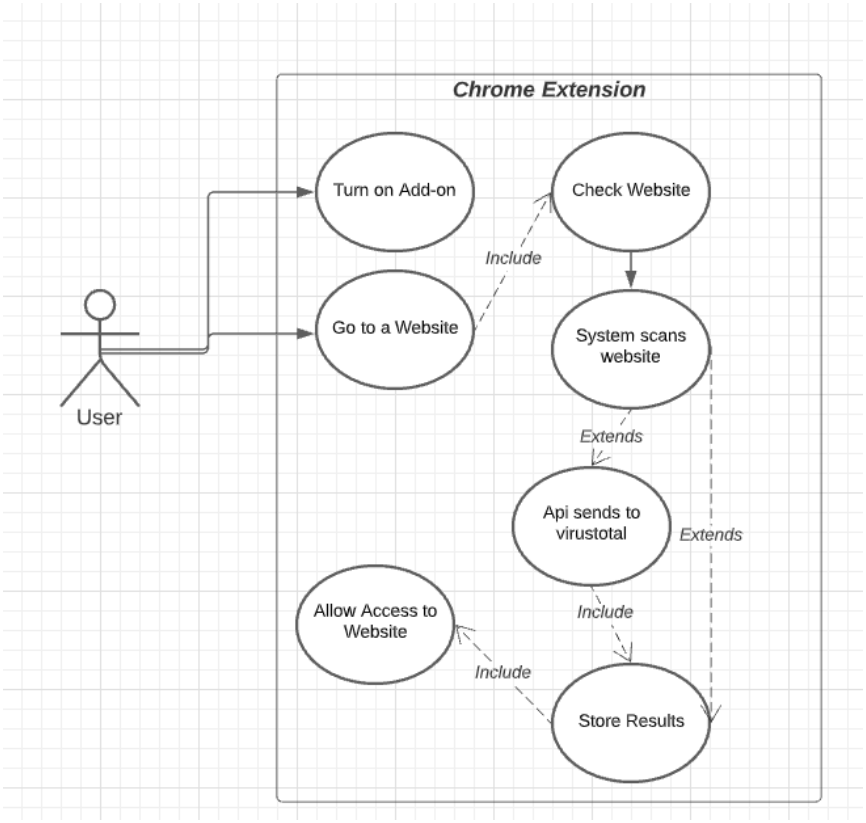
Use Case Diagram

When User Access a Fake/Fraudulent Website(reverse Extend arrows)



- The user downloads and enables the chrome extension.
- With the extension turned on they go to visit a website.
- Once they enter a website the extension will procced with its check
- The extension itself will scan the website
- If the extension itself can't find anything wrong with the website, it will then send it to a virus scanner like "virus total" using an API to make sure if the website is legitimate.
- It will then collect and store the results and it will look at the results
- If the results show that the website is fake, then the extension will block access to the website and warn the user.

When a user accesses a legitimate website. (reverse Extend arrows)



- The user downloads and enables the chrome extension.
- With the extension turned on they go to visit a website.
- Once they enter a website the extension will procced with its check
- The extension itself will scan the website
- If the extension itself can't find anything wrong with the website, it will then send it to a virus scanner like "virus total" using an API to make sure if the website is legitimate.
- It will then collect and store the results and it will look at the results
- If the results show that the website is legitimate, then the extension will allow access to the website.

Metrics

In order to gauge if my project was success this is the list, I made for it

- **Does the Add-on block access to a fake website?**
- **Does the Add-on allow access to a legitimate website?**
- **Is it easy to use?**
- **Is it too intrusive?**

Is there a precedent for this application?

There are applications and add-ons that exist and are similar to my add-on, some of which include “Avira Browser Safety” which is an add-on that I am familiar as I am using it myself, it blocks the user from phishing and malicious websites and it also has other uses like it block malicious ads and prevents companies from tracking you. Another application/add-on that is similar to my add-on is “Web Titan” which is an add-on that prevents users from accessing malicious and phishing websites and it use its own web filtering to achieve this.