

# Chapter 5

## Design

### 5.1 Architecture

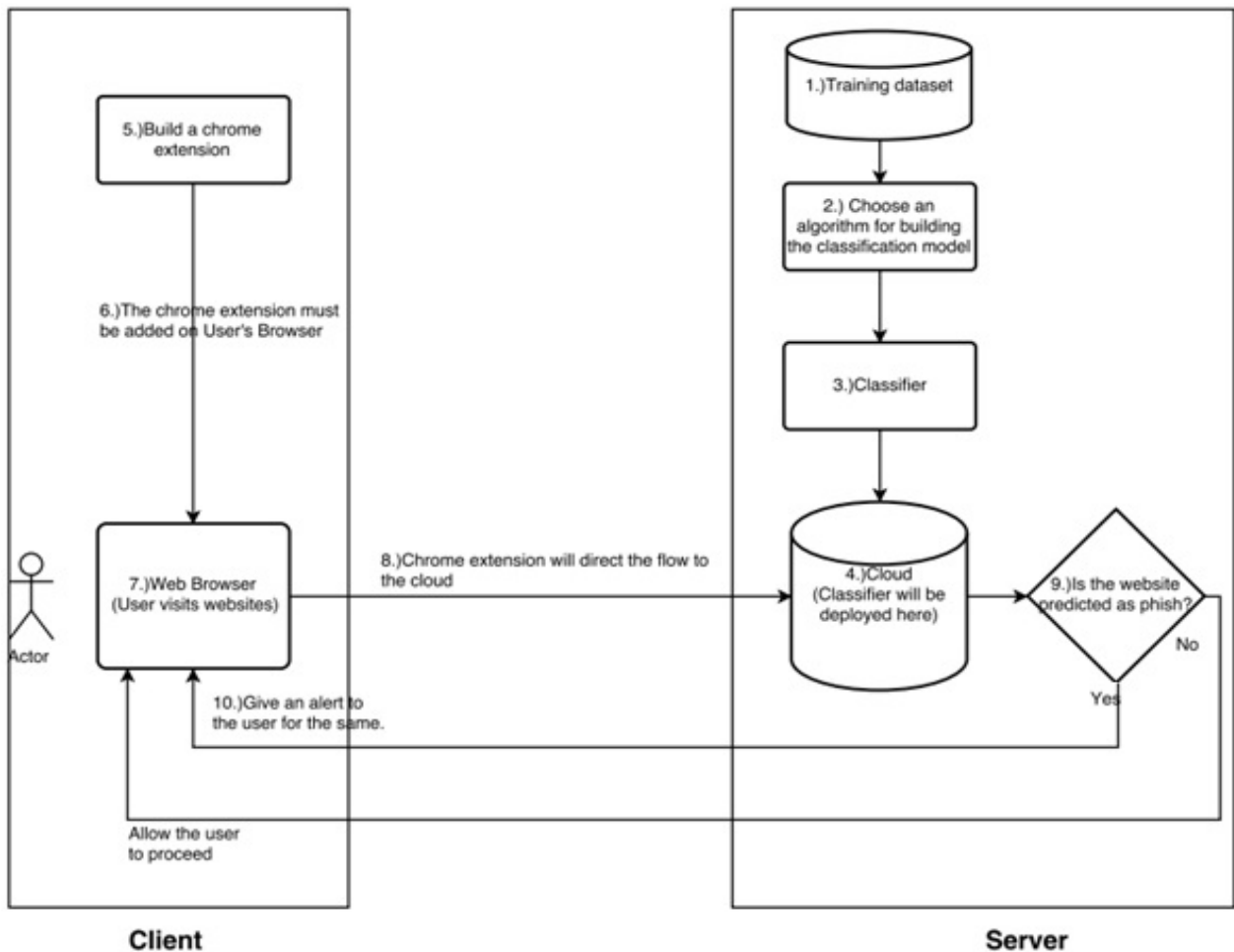


Figure 5.1.1: Architecture design of the system

When the client visits the browser, it requests for a URL from the browser. This requested URL is fetched by the chrome extension. The chrome extension also extracts the URL attributes such as URL based features, Lookup based features, Search Engine based features, HTML DOM based

features, Certificate based features and Website Traffic features. This extracted URL attributes act as test data for the classifier deployed on the cloud. The classifier model will be trained on a dataset of phishing websites and will test the newly entered or newly generated URLs by performing the chosen algorithm.

The classifier will either predict the entered URL as malicious website or it will predict it as a safe website. If it is a phished website then the user will be alerted that if they proceeded further on this URL their credentials are at risk of getting hacked and if it is a safe website then the user can carry out further processing on that page.

## 5.2 User Interface Design

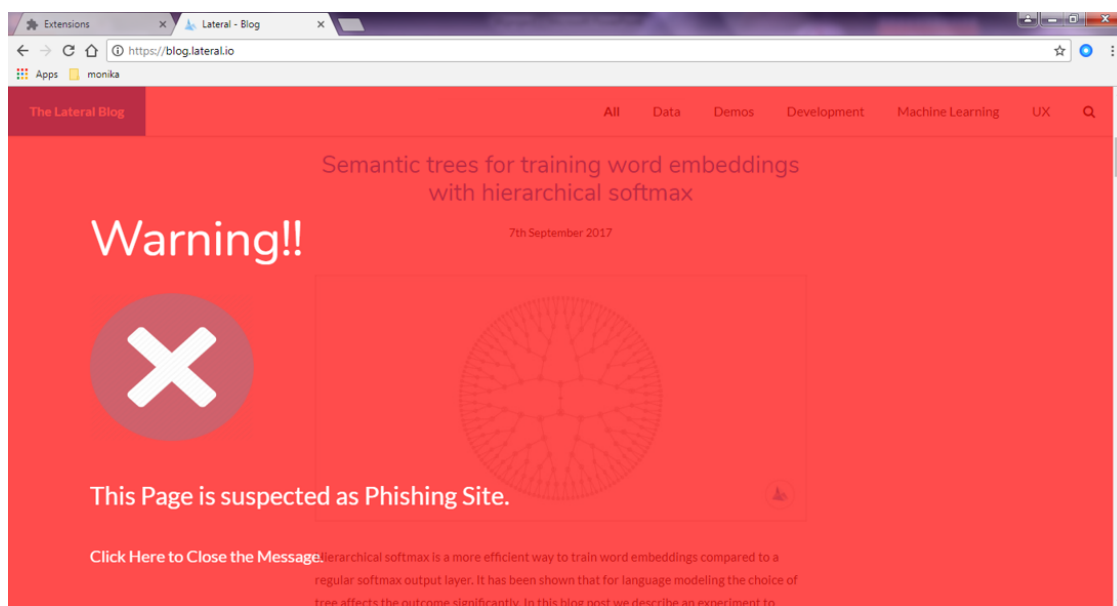


Figure 5.2.1: Warning message for a phishing site

Figure 5.2.1 shows the warning message that will be shown to the user when he/she visits a phishing site. The webpage is overlaid by the warning message and alerts the user that the webpage is not safe to visit. But if the user still wants to view the page, he/she can click the link to close the message and ignore the same.

**Detailed working of the Chrome Extension:**

The output generated in figure 5.3.1 is an alert given to the user through the chrome extension. The Chrome extension is an intermediary between the user and the system.

For our system to work, our chrome extension must be added on the users web browser. When the user visits a website, the Chrome extension fetches that URL. Furthermore, it decomposes the URL into various attributes like-

- Having\_IP\_Address
- Having\_at\_Symbol
- URL\_length
- Port
- HTTPS\_Token
- DNS\_Record
- PageRank
- Age\_of\_Domain

These extracted attributes are then sent on the cloud where the trained model is deployed. After the model tests these URL attributes and predicts the website as safe or phished, the result is sent to the Chrome extension which alerts the user. Our systems task ends here and after this it is completely up to the user to carry out the websites proceeding.