

Asia Pacific College School of Computing and Information Technology Magallanes, Makati City

IDENTIFYING FAKE NEWS ON SOCIAL MEDIA WEBSITES

Project Documentation Submitted to the Faculty of School of Computing and Information Technologies of Asia Pacific College

by

Marc Anthony Nares
Aleo De Leon
Joshua Cruz
Wyatt Holgado
BSCS-SS / SS152

to

Mr. Manuel Sebastian Sanchez

Contents

Coi	ntents	2
	stract	
	Introduction	
	roject Context	
	Purpose and Description	
	Dijectives	
	cope and Limitations	
	Review of Related Literature	
III.	Technical Background	9
	Design and Methodology	
VI.	Conclusions and Recommendation	12
VII.	References	13

Abstract

This document circles around fake news on the internet. In this research the researchers will

create a model that identifies if a link posted on social media sites leads to an article that is fake or not.

The researchers will use an algorithm for classifying the link and it will be implemented through a web

extension that will only run on social media sites. Considering that there are various ways in identifying

fake news, this document will be providing the characteristics of fake news and how accurate is the

algorithm in identifying fake news.

KEYWORDS: Fake news, classification

I. Introduction

Project Context

Fake news is a deliberate misinformation or hoax that spreads via traditional print, broadcast news media or online social media (Novotny, 2017). It misleads people and make the world less informed. It harms the community and the industry in an alarming level (Stecula, n.d.).

Eric Trump, the son of Donald Trump, tweeted an article about paid protestors from the domain "abcnews.com.co" that reinforced right wing conspiracy theories. The article was completely fabricated, but it resembled the real ABC News enough to fool those who weren't paying attention (Palmisano, 2016). With the way on how fake news is spreading, it would be ideal to have application that help identify fake news online.

Purpose and Description

The main purpose of this project is to give awareness to online users from being tricked by fake news. The proponents will create an algorithm that can identify fake news in social media sites. It will be implemented through an extension that will work only on Google Chrome and it will only identify fake news in social media sites.

Objectives

The objectives of this study are:

- 1. To create a classification model that determine whether a link leads to a fake news article or not.
- 2. To create a web extension that can identify whether a link clicked by a user leads to a fake news article or not.

Scope and Limitations

The study is about identifying fake news. The researchers will use JavaScript, HTML, PHP, CSS programming languages to create a web extension for identifying fake news. The gathered datasets will come from three online websites (Kaggle.com, cbcpwebsite.com, Primer.com). The web extension will only work on the latest and upcoming versions Google Chrome and it will not work on any other browsers.

This study is only limited in identifying fake news on microblogging sites and it will not identify fake news on other sites.

II. Review of Related Literature

In this chapter, the researchers will be presenting an articles and related readings about this study. Moreover, this chapter suggests about fake news, web extension or plugin. Furthermore, this chapter will also inform that the researchers aims to create a web extension that will scan the links for fake news.

Fake News

According to Ruchansky et al. (2017), they study about the problems of fake news detection. The researchers read several articles that addressed the problem by focusing on the text, the response an article receives, or the users who source it. They claim that it is important to combine all three. They propose the CSI model which is composed of three modules. First module, Capture, captures the abstract temporal behavior of user encounters with articles, as well as temporal textual and user features, to measure response as well as the text. The second is score; it estimates a source suspiciousness score for every user, which is then combined with the first module to produce a predicted label for each article. The separation into modules allows CSI to output a prediction separately on users and articles, incorporating each of the three characteristics, resulting into combining the information for classification. The model demonstrated the accuracy of CSI in classifying fake news articles.

Badaskar et al. (n.d.) focused on the topic about fake news. The researcher measures the accuracy of number of articles that are classified correctly as real or fake and the log-probability that measures the classification decision, the researchers used a classification-task based formalism for evaluating various features with the objective of improving conventional language models. Features that perform well in the task for classifying real and fake articles. These features are syntactic, semantic and empirical. The semantic features contribute significantly to the classification task accuracy.

McIntire (2017) conducted a study on a model that fake news articles could classify accurately. He tested his model in his fake news datasets. Remarkably, it was able to correctly identify them as fake. But It turns out that his hypothesis predicting model would struggle at classifying news articles was quite wrong. McIntire thought that it would be excellent and managed to surpass that by a significant margin.

McIntire created a model that convinced that it is as good as it appears. To understand why this might have happened, McIntire takes a look at the fakest and realest words in the data. Using a technique that the researcher borrowed from Kevin Markham (author) First he started off with a table two columns wide and 10558 rows long. The first column represented how many times a given word appeared in articles classified as fake and the second column was how many times a word appeared in a real article. Then he divided the fake column by the total number of fake articles the model classified and so on for the real column. Next, added the number one to every value in the data because he created a new column of Fake:Real ratios and didn't want to get an error by dividing zero. This Fake:Real is a pretty good but by no means perfect metric of just how fake or real a certain word. The logic is pretty simple, if a word shows up a lot of fake articles and rarely in real articles then its fake to real ratio will score be pretty high. In addition, McIntire (2017) think that a standard Naive Bayes text classification model can help and provide insight into addressing the issue, a more powerful tool should be employed to fight fake news (McIntire, 2017).

Verstraete (2016) conducted a study entitled 'Identifying and Countering fake news'. The researchers presented a study that addresses a useful classification of fake news based on their creators' intent to deceive and motivation. In particular, it identifies four key categories: satire, hoax, propaganda, and trolling. This analytical framework will help policymakers and commentators alike by providing accuracy to debates over the issue. The study identifies key structural problems that make it difficult to design interventions that can address fake news effectively. These include the ease with which authors can produce user generated content online. Authors often have a mixture of motives in creating content, making it less likely that a single solution will be effective. Consumers of fake news have limited incentives to invest in challenging or verifying its content, particularly when the material supports their existing beliefs and perspectives. Finally, the researchers said that fake news rarely appears alone it is frequently mingled with more accurate stories, such that it becomes harder to categorically reject a source. Then, the report classifies existing and proposed interventions based upon the four regulatory modalities catalogued by Larry Lessig; Law, code, social norms and markets. It assesses the potential and

shortcomings of extant solutions. The most important is the study offers a set of model interventions, classified under the four regulatory modalities, to generate discussion and to provide a starting point for policymakers who want to reduce the effects of fake news. The goal of researchers is to create a foundation to help advance dialogue about fake news and to suggest tools that might mitigate it (Verstraete, 2016).

The researchers will conclude that these articles will help them to learn more about web browser extensions and fake news that will apply to the study about identifying fake news using web extension.

III. Technical Background

Web Extension

Extensions are bits of code that modify the functionality of a web browser. They are written using standard Web technologies - JavaScript, HTML, and CSS - plus some dedicated JavaScript APIs. Among other things, extensions can add new features to the browser or change the appearance or content of particular websites. Basically, the researchers will create an extension that can identify fake news in social media sites.

IndexedDb Database

A collection of data is called a Database. In order to manage a data in a database, it will need to have a Database Management System (DBMS). DBMS can help the user interact with the database itself and it can also help them to handle and capture the data. The researchers will use IndexedDb. IndexedDB is a low-level API for client-side storage of significant amounts of structured data, including files/blobs. This API uses indexes to enable high performance searches of this data.

JavaScript

JavaScript is a programming language that enables you to create dynamically updating content, control multimedia, animate images, and pretty much everything else. The researchers will use this language to create an extension.

IV. Design and Methodology

A web extension is a plug-in that extends the functionality of a web browser. The researchers will create a web extension that can identify fake news and will only run if the link is clicked. When the link is clicked, the system will compare the news link article from the list of fake news links and from the list of authentic news gathered by the team. The data for fake and authentic news list will be gathered from kaggle.com, CBCP (Catholic Bishops' Conference of the Philippines,Primer.com) and it will be saved in a database. If the link is not in the list, the system then will rate the following from 1-5(See Figure 1 for reference) depending on how positive they are in specific factors. After rating the article the system will compute for the average and the score will be compared to our rating scale.

- A. How reliable is the source (Depend on domain name and where you have found the article)
- B. Rate the author itself, is the author have enough legibility? Is he famous? Have he published anything else?
- C. Title: unusual formatting
- D. The availability of the article from other media, Is the information or related articles available on the other sites or medias?

ARTICLE 1: DUTERTE TO THROW OPPOSITION SENATORS IN MANILA BAY AS PART OF GOVERNMENT CLEAN UP from adobochornicles.com

ARTICLE 2: DUTERTE'S SECOND SONA COULD TAKE 1.5 HOURS- MALACANANG from gmanetwork.com

	А	В	С	D
ARTICLE1	2	1	4	3
ARTICLE2	5	4	5	5

Strongly				Strongly
Disagree	Disagree	Neutral	Agree	Agree

Figure 1 (1 2 3 4 5)

6

After comparing the link and classifying it the data will be saved to database for future preference. If the author is unknown the system will automatically flagged it as fake. If the link is confirmed fake the system will notify the user with a dialog box popped up, but if the link article is authentic the system will also notify the user.

The extension will be developed using HTML, CSS, PHP and JavaScript and it will be compatible to Google Chrome.

VI. Conclusions and Recommendation

Fake news can be lessened or better yet eliminated, since people keep falling prey for such posts; it needs to be stopped. This paper is meant to do just that; the program we are proposing is meant to detect if the news posted in your social media websites, which would literally get marked as a fake if it is one. To identify a fake news one must check the author, URL, title, and the availability of the article from other medias. This program will be a plugin for the users' internet browsers, but will only work for social media sites, and will not detect if posted news are fake from other websites. If this program could be implemented, there will definitely be a big change in how news would be spread, since users will no longer fall for faulty news articles and posts.

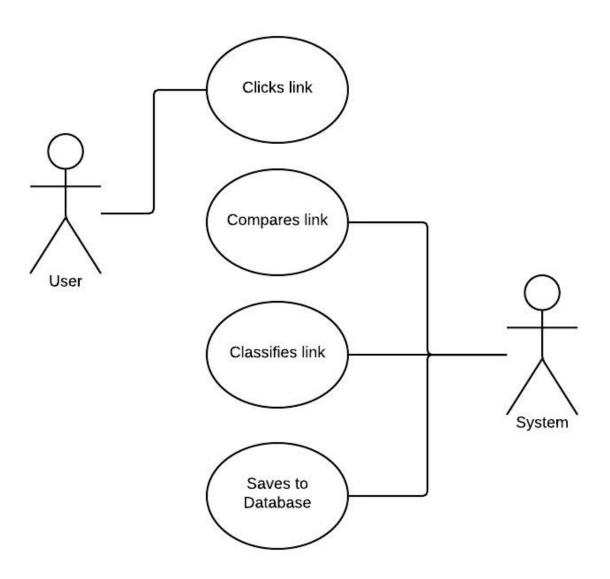
To help increase the accuracy of the extension, the researchers recommend to add more features for classifying data and to work not only in chrome but also on other browsers.

VII. References

- Dezyre. (2017, June 20). Retrieved from dezyre: https://www.dezyre.com/article/top-10-machine-learning-algorithms/202
- Eugene Kiely, L. R. (2016, November 18). *FactCheck.org*. Retrieved from http://www.factcheck.org/2016/11/how-to-spot-fake-news/
- Greg. (2017, January 24). *yhat*. Retrieved from yhat: http://blog.yhat.com/posts/why-support-vector-machine.html
- IBM. (n.d.). Retrieved from IBM knowledge center: https://www.ibm.com/support/knowledgecenter/en/SS3RA7_15.0.0/com.ibm.spss.modeler.help/s vm howwork.htm
- Machine Learning 101. (n.d.). Retrieved from Medium: https://medium.com/machine-learning-101/chapter-2-svm-support-vector-machine-theory-f0812effc72
- Mark Verstraete1, D. E. (n.d.). *Identifying and Countering fake news*. Retrieved from https://webcache.googleusercontent.com/search?q=cache:JZsN3vbXxE4J:https://law.arizona.ed u/sites/default/files/asset/document/fakenewsfinal.pdf+&cd=2&hl=en&ct=clnk&gl=ph
- McIntire, G. (n.d.). *Machine Learning Finds "Fake News" with 88% Accuracy*. Retrieved from KDnugget: http://www.kdnuggets.com/2017/04/machine-learning-fake-news-accuracy.html
- Media Insight Project. (2016, March 17). *American Express Institute*. Retrieved from https://www.americanpressinstitute.org/publications/reports/survey-research/trust-news/
- Novotny, E. (2017, August 1). PennState. Retrieved from libraries.
- Palmisano, S. (2016, December 29). *EagleNews*. Retrieved from eaglenews: http://eaglenews.org/opinion/fake-news-leads-to-real-problems/
- Rappler. (2017, April 10). Retrieved from http://www.rappler.com/technology/social-media/166326-how-to-spot-fake-news-facebook
- Sathyanarayana, S. V. (n.d.). Data classification using Support vector. *Data classification using Support vector*.
- stackexchange. (n.d.). Retrieved from crossvalidated:
- https://stats.stackexchange.com/questions/23391/how-does-a-support-vector-machine-svm-work *Stackexchange*. (n.d.). Retrieved from ComputerScience:
- https://cs.stackexchange.com/questions/10304/which-classifier-is-more-accurate-for-a-symclassification
- Stecula, D. (n.d.). *The conversation*. Retrieved from theconversation: http://theconversation.com/the-real-consequences-of-fake-news-81179

DIAGRAMS

Use Case Diagram



Use Case Full Description

Circles the lank		ll Description
Description The user clicks the link in his/her Facebook newsfeed. 1. User clicks the link. 2. The system runs. 3. Use case ends. Pre-condition The user should click the link. Post-condition The system will run Comparing detected link. Actor. System Description: The system will compare the detected links. Flow of Events. 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The system compared the detected link. Post-Condition: The system compared the detected link. Actor: System Description: The system will classify the detected links. Flow of Events. User clicks the link 1. The system should closely whether the compared link is fake or not. 2. Use case ends.	Use Case	Clicks the link
Procondition	Actor:	User
2. The system runs. 3. Use case ends. Procondition The user should click the link. Post-condition The system will run Use Case: Comparing detected link Comparing detected link Description The system will compare the detected links. Flow of Events: 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pro-Condition: The user should click the link. Post-Condition: The system compared the detected link. Use Case: Caseliying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User cicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pro-Condition: The system should compare the link.	Description	The user clicks the link in his/her Facebook newsfeed.
Pre-Condition: The system will run Use Case: Comparing detected link Actor: System Description: The system will compare the detected links. Flow of Events: 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The user should click the link. Post-Condition: The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. The system should compare the link.	Flow of Events	2. The system runs.
Use Case: Comparing detected link Actor: System Description: The system will compare the detected links. 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The user should click the link. Post-Condition: The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. The system should compare the link.	Pre-condition Pre-condition	The user should click the link.
Actor: System Description: The system will compare the detected links. Flow of Events: 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The user should click the link. Post-Condition: The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Post-condition	The system will run
Description: The system will compare the detected links. 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The user should click the link. The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Use Case:	Comparing detected link
Flow of Events: 1. The system request data from database 2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The user should click the link. Post-Condition: The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Actor:	System
2. The system compares the detected link to the list of fake/authentic news in database. 3. Use case ends. Pre-Condition: The user should click the link. Post-Condition: The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. User case ends. Pre-Condition: The system should compare the link.	Description:	The system will compare the detected links.
Post-Condition: The system compared the detected link. Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Flow of Events:	2. The system compares the detected link to the list of fake/authentic news in database.
Use Case: Classifying detected link Actor: System Description: The system will classify the detected links. User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Pre-Condition:	The user should click the link.
Actor: System Description: The system will classify the detected links. Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Post-Condition:	The system compared the detected link.
Description: The system will classify the detected links. User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Use Case:	Classifying detected link
Flow of Events: User clicks the link 1. The system will classify whether the compared link is fake or not. 2. Use case ends. Pre-Condition: The system should compare the link.	Actor:	System
The system will classify whether the compared link is fake or not. Use case ends. Pre-Condition: The system should compare the link.	Description:	The system will classify the detected links.
	Flow of Events:	The system will classify whether the compared link is fake or not.
Post-Condition: The system classified the detected link.	Pre-Condition:	The system should compare the link.
	Post-Condition:	The system classified the detected link.

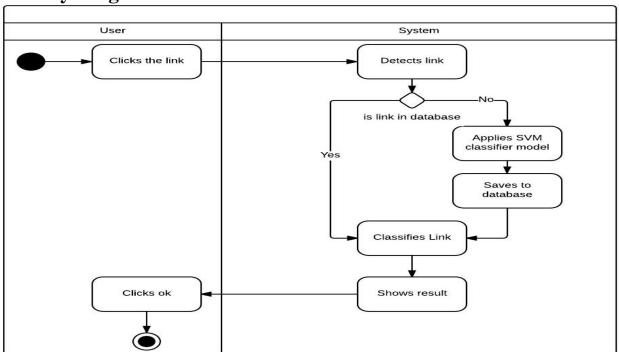
Use Case Full Description

CBC CMBC I G	ose case I an Description				
Use Case:	Save to database				
Actor:	System				
Description:	The system will save the classified link to the database.				
Flow of Events:	The system will save the classified link in database Use case ends.				
Pre-Condition:	The system must classify the link				
Post-Condition:	The system saves the classified link to the database.				

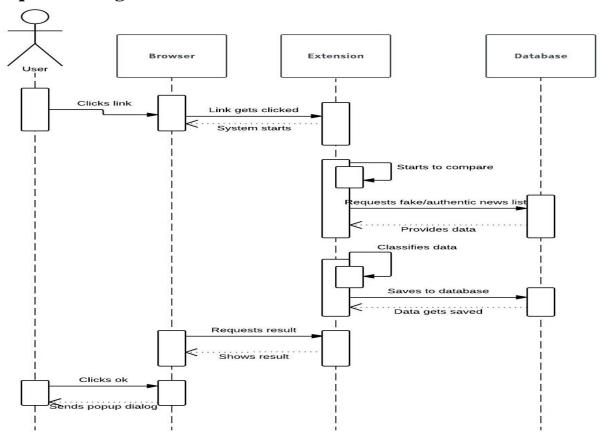
Event Table

Event	Trigger	Source	Use Case	Response	Destination
User clicks the link	link was clicked	User	Clicks link	System runs	System
System compares link	System compares the link	System	Compares link	System compares the link to the list of fake news links	System
System classifies the link	System classifies the link	System	Classifies link	System classifies the link	System
System saves to database	System saves to database	System	Saves to database	The classified link is saved to database	Database

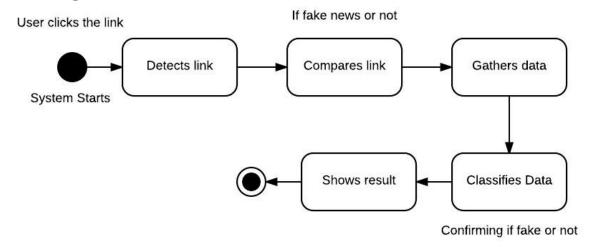
Activity Diagram



Sequence Diagram

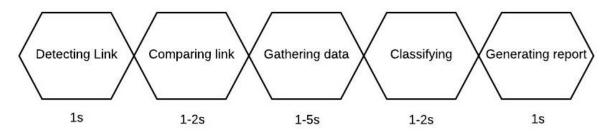


State Diagram

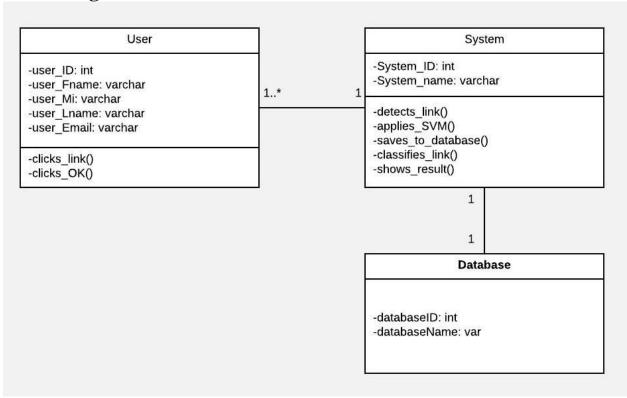


Timing Diagram

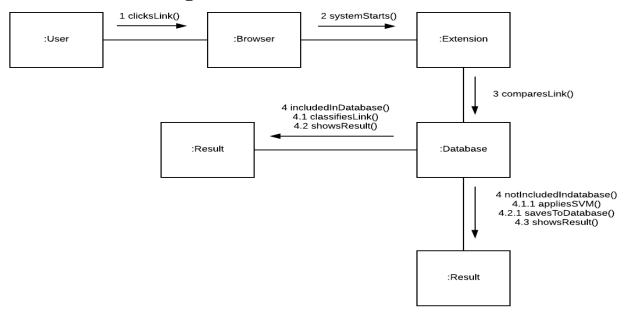
Process time may vary based on computer hardware



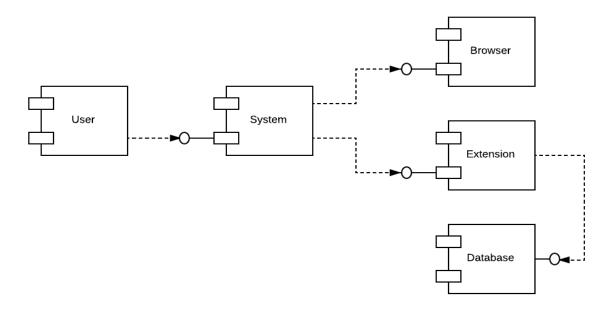
Class Diagram



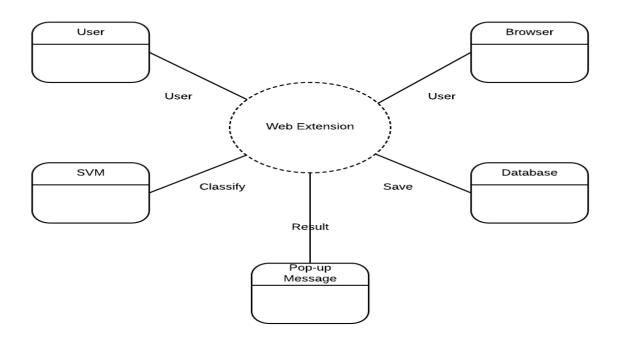
Communication Diagram



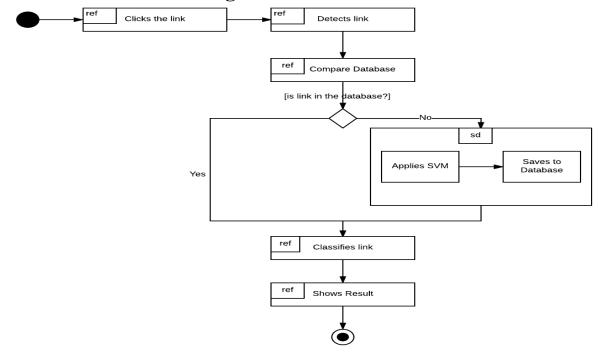
Component Diagram



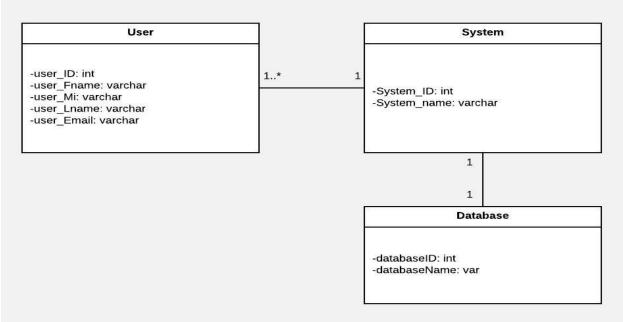
Composite Diagram



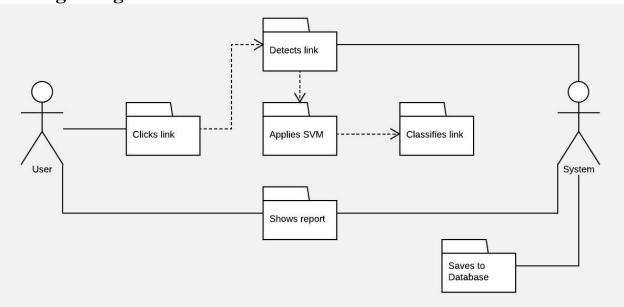
Interaction Overview Diagram



Object Diagram



Package Diagram



Deployment Diagram

