AI User Safety Application

Project Abstract

By

CMPE 295B

Gulnara Timokhina (**gulnara.timokhina@sjsu.edu**)
Mirsaeid Abolghasemi (**mirsaeid.abolghasemi@sjsu.edu**)
Varun Bhaseen (**varun.bhaseen@sjsu.edu**)

Project Advisor

Professor Vijay Eranti

Date: May 7, 2021

ABSTRACT

AI User Safety Application

By

Gulnara Timokhina, Mirsaeid Abolghasemi, Varun Bhaseen

A user's privacy protection is of prime importance nowadays. The majority of user privacy violations happen through phishing attacks. As per the reports published by the "Anti-phishing working group for Q4 2020", it has been observed that the number of phishing sites detected was 637,302 of which 84% now use Secure Sockets Layer (SSL) protection. A phishing attack can be detected from paid or freeware anti-virus software, corporate email phishing detection, and user intelligence or awareness.

The primary goal of a phishing attack is to exploit human weaknesses. The challenge with current phishing detection is the lack of availability of a reliable state-of-art tool that could compensate for these weaknesses. The majority of phishing detection technology is based on a classical approach where the agent (detector) relies on information on which it has been trained. The agent does not factor into a real-time artificial intelligence-based detection that can detect the most recently evolved techniques on which phishing attacks are based. Also, most commercial applications are highly resourced intensive on memory footprint and CPU usage. There are no quick, small, and reliable solutions in the market.

In this project, we are proposing an artificial intelligence-based real-time detector that can protect user's privacy details by constantly scanning a web page for malicious scripts, phishing contents, domain authenticity, and logo identifiers. Our approach uses not only natural language processing but also computer vision to detect the authenticity of the web page and the use of logos or images on that web page. The outcome is a plugin on a browser that can consume minimal resources and can give a quick scan notification about the safety of the web page.