AI User Safety Application

Project Abstract

By

CMPE 295W

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

Project Advisor

Professor Vijay Eranti

Date: September 1, 2020

ABSTRACT

AI User Privacy 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 "*Anti-phishing working group for Q2 2020*", it has been observed that the number of phishing sites detected was 146,994 of which 78% now use SSL protection. Whereas with the Covid-19 pandemic of 2020, the number of social media platform users has been increased along with a surge of 20% (from Q1 2020) in phishing attacks. 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 in 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 which 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 which can detect the most recent evolved techniques on which phishing attacks are based.

In this project, we will be 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 will be using not only NLP 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 will be to run a plugin on a browser that can consume minimal resources and can give a quick scan notification about the safety of the web page.