InApp

Computer Society of India™
Trivandrum Chapter

ACADEMIC PARTNER
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

12TH CSI-InApp INTERNATIONAL STUDENT PROJECT AWARDS | 2023

WIN! ₹50,000

CONSOLATION PRIZE ₹25,000

Cash prizes and placement opportunity for all finalists!

PROJECT ID

CSIN2023-01

PROJECT TITLE

CYBER HYGIENE TOOL - KAVACH

PROBLEM DEFINITION

Internet usage has become an integral part of our lives, and with it comes the risk of cyber threats. However, despite the growing awareness about cyber threats, many internet users remain unaware of the risks associated with their online activities. This naivety puts them at risk of falling victim to scams and frauds that can lead to significant financial losses.Recent studies have estimated that global cyber security threats may reach a staggering 10 trillion dollars. Unfortunately, there is no single solution that can fully protect internet users from these threats. As a result, many people remain susceptible to cyber-attacks, making it crucial to promote cyber hygiene awareness and educate people about safe internet practices.This abstract outlines the problem of the lack of cyber hygiene awareness among Indian internet users and the risks it poses. It highlights the need to promote awareness and implement protocols to safeguard users against cyber-attacks. Through research and analysis, we hope to identify the root causes of this problem and propose solutions that will help users protect themselves online. Our goal is to create a safer online environment for global internet users and reduce the risks associated with their online activities.

PROPOSED SOLUTION

To address the problem of the lack of cyber hygiene awareness among Indian internet users and the increasing risks associated with online activities, we have developed a comprehensive solution called KAVACH. KAVACH is an AI-based advisory tool that provides users with a one-stop solution to safeguard their online activities. It keeps track of all online activities and provides real-time alerts and suggestions to users, enabling them to make informed decisions about their online behavior.KAVACH uses federated learning models to improve its algorithms continuously. By utilizing deep neural networks, it identifies complex types of attacks and classifies them for the users, ensuring a safer online experience.Moreover, to ensure users' privacy and security, KAVACH uses a sandboxing agent that tests the product before deploying it onto users' devices. This approach enables us to detect and prevent malware attacks and prevent cybercriminals from accessing users' confidential information.KAVACH is designed to meet the needs of users of all skill levels, making it easy for anyone to use it. Our ultimate goal is to create a safe online environment for Indian internet users and prevent them from falling victim to cyber-attacks. With KAVACH, we believe we can make a significant impact in promoting cyber hygiene awareness among Indian internet users and keep them safe online.

INNOVATION ASPECT IN THE PROPOSED SOLUTION

* A system and method for providing artificial intelligence based cyber hygiene framework.

* An artificial intelligent based advisory service to the users to help them avoid potentially dangerous web sources.

* A globally coordinated dynamic federated learning framework which continuously fine tunes its response to globally observed threats.

* A feedback mechanism which helps improve accuracy and effectiveness of the advisories , issued by the AI based agent on individual computers , against new emerging threats.

* A multidimensional framework protecting user against a multitude of online frauds and threats.

* A framework providing access to genuine web sources foe downloading commonly-used software/content.

SPECIFIC OUTPUTS OF THE PROJECT

* AI based agent deeply classifies the web urls and classifies them for further processing.

* An advisory/recommendation system for the genuine web portal / sources for downloading commonly-used software/content.

* Sandboxed Environment to check for malformed or malicious data propogation.

* A global Artificial intelligent Federated Learning based model that updates each and every product distribution with an attack incident.

* A Black list and a while list is maintained globally in order to safeguard every other user from any type of attack.

TECHNOLOGY AND PLATFORM

Chrome Extension - Javascript , Jquery (For the Consumer side application interface)

Web App - Django (For building the Aritifcial Intelligent model)

AI Models - Federated learning models , Deep CNN (Convocational Neural Networks) models

Database - AWS / Mongo DB (For A global White and a BLack List)

CURRENT STATUS OF IMPLEMENTATION

The user side interface is implemented with functionalities like advisory systems for the genuine web portals or the sources , Malicious services discovery on the network and malicious content detection systems , web url parsing and classifications system , Phishing links and Dark web portals Detection systems.

DETAILS

Name of the College	MODEL INSTITUTE OF ENGINEERING AND TECHNOLOGY

TEAM DETAILS

Guide Name	Prof. Ankur Gupta	Designation	Director, MIET Jammu
Email	ankurgupta@mietjammu.in	Phone	9797522100
Team Leader Name	Aadhaar Koul	Branch and Semester	CSE - 6th
Email	2020a1r040@mietjammu.in	Phone	6005846156