**AN INDUSTRY ORIENTED MINI PROJECT REPORT ON**

**SAFESURF-Chrome Extension**

*in the partial fulfillment of the requirements for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

in

**CSE (Cyber Security)**

**Submitted by**

**E SRIMANI TEJA 22B81A6251**

**T VIVEKANANDA22B81A6263**

**K VIGNESHWAR22B81A6260**

Under the guidance of

**G SAHITHI**

**Assistant Professor**

****

**DEPARTMENT OF CSE(Cyber Security)**

**CVR COLLEGE OF ENGINEERING**

**(*An Autonomous institution, NAAC Accredited and Affiliated to JNTUH, Hyderabad*)**

Vastunagar, Mangalpalli (V), Ibrahimpatnam (M),  
Rangareddy (D), Telangana- 501 510

**CVR COLLEGE OF ENGINEERING**

**(*An Autonomous institution, NAAC Accredited and Affiliated to JNTUH, Hyderabad*)**

Vastunagar, Mangalpalli (V), Ibrahimpatnam (M),  
Rangareddy (D), Telangana- 501 510

**DEPARTMENT OF CSE (Cyber Security)**

****

**CERTIFICATE**

This is to certify that the Industry Oriented Mini Project report entitled **“SAFESURF-Chrome Extension”** Bonafide record of work carried out by **E SRIMANI TEJA(22B81A6251), T VIVEKANANDA(22B81A6263)** and **K VIGNESHWAR(22B81A6260)**submitted to **Dr. C. Raghavendra, Associate Professor** for the requirement of the award of **Bachelor of Technology** in **CSE (Cyber Security)**to the CVR College of Engineering, affiliated to Jawaharlal Nehru Technological University, Hyderabad during the year 2024-2025.

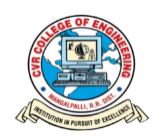
**Project Guide Project Coordinator**

**G. Sahithi**  **Dr. C. Ragahavendra**

Assistant Professor Associate Professor

Department of CSE(CS) Department of CSE(CS)

**Head of the Department External Examiner**

**CVR COLLEGE OF ENGINEERING**

(UGC Autonomous Institution)

Affiliated to JNTU Hyderabad

Vastunagar, Mangalpalli (V), Ibrahimpatnam (M),

Ranga Reddy (Dist.), Hyderabad – 501510, Telangana State

**DECLARATION**

We hereby declare that the Industry Oriented Mini Project report entitled **“SAFESURF-Chrome Extension”** is an original work done and submitted to CSE (Cyber Security) Department, CVR College of Engineering, affiliated to Jawaharlal Nehru Technological University Hyderabad in partial fulfilment for the requirement of the award of Bachelor of Technology in CSE (Data Science) and it is a record of bonafide project work carried out by us under the guidance of **G. SAHITHI,** Assistant Professor, Department of CSE (Cyber Security).

We further declare that the work reported in this project has not been submitted, either in part or in full, for the award of any other degree in this Institute or any other Institute or University.

Signature of the Student

**E SRIMANI TEJA**

Signature of the Student

**T VIVEKANANDA**

Signature of the Student

**K VIGNESHWAR**

**Date:**

**Place:**

**ACKNOWLEDGEMENT**

We are thankful for and fortunate enough to get constant encouragement, support, and guidance from all **Teaching staff of CSE (Cyber Security) Department** which helped us in successfully completing this Industry Oriented Mini Project.

We are extremely thankful to our internal guide **G. Sahithi,** Assistant Professor, Department of CSE (Cyber Security) for providing support and guidance, which made us complete the Industry Oriented Mini Projecton time.

We thank **Dr. C. Raghavendra**, Project Coordinator and **Mrs. G. Sahithi, Mrs. A. Geetha,** Project Review Committee members for their valuable guidance and support which helped us to complete the Industry Oriented Mini ProjectWork successfully.

We thank Professor and Head of the Department **Dr**. **M. Sunitha,** for giving us all the support and guidance, which made us to complete the Industry Oriented Mini Project duly.

We would like to express heartful thanks to **Dr. H. N. Lakshmi,** Associate Dean, ET Department, for providing us an opportunity and extending support and guidance.

We thank our Vice-Principal **Prof. L. C. Siva Reddy** for providing excellent computing facilities and a disciplined atmosphere for doing our work.

We wish a deep sense of gratitude and heartfelt thanks to our Principal **Dr. K. Rama Mohan Reddy** and the **Management** for providing excellent lab facilities and tools.

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Chapter No.** | | **Contents** | **Page No.** |
|  |  | List of Tables | i |
|  |  | List of Figures | ii |
|  |  | List of Symbols | iii |
|  |  | Abbreviations | iv |
|  |  | Abstract |  |
| 1 |  | **Introduction** |  |
|  | 1.1 | Motivation |  |
|  | 1.2 | Problem Statement |  |
|  | 1.3 | Project Objectives |  |
|  | 1.4 | Project Report Organization |  |
| 2 |  | **Literature Survey** |  |
|  | 2.1 | Existing work |  |
|  | 2.2 | Limitations of Existing work |  |
| 3 |  | **Software & Hardware specifications** |  |
|  | 3.1 | Software requirements |  |
|  | 3.2 | Hardware requirements |  |
| 4 |  | **Proposed System Design** |  |
|  | 4.1 | Proposed methods |  |
|  | 4.2 | Class Diagram |  |
|  | 4.3 | Use case Diagram |  |
|  | 4.4 | Activity Diagram |  |
|  | 4.5 | Sequence Diagram |  |
|  | 4.6 | System Architecture |  |
|  | 4.7 | Technology Description |  |
| 5 |  | **Implementation & Testing** |  |
|  | 5.1 | Front page Screenshot |  |
|  | 5.2 | --- |  |
| 6 |  | **Conclusion & Future Scope** |  |
|  |  | **References** |  |
|  |  | **Appendix: (If any like Published paper / source code)** |  |

**List of Tables**

|  |  |  |
| --- | --- | --- |
| **Table No.** | **Title** | **Page No.** |
| 3.1 | Values Assigned to Standard kε Turbulence Model Coefficients | 55 |
| 3.2 | Values Assigned to RNG kε Turbulence Model Coefficients | 57 |
| 4.1 | Engine Specifications | 90 |
| 4.2 | Geometrical Details of the Injector | 92 |
| 4.3 | Boundary and Initial Conditions | 94 |
| 4.4 | Grid Independence Study | 99 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Title** | **Page No.** |
| 3.1 | Lagrangian Droplet Motion | 70 |
| 4.1 | Vertical Manifold | 95 |
| 4.2 | 200 Bend Manifold | 97 |
| 4.3 | 900 Bend Manifold | 99 |
| 4.4 | Spiral Manifold | 100 |
| 4.5 | Spiral Manifold Configuration | 100 |

**SYMBOLS**

Symbols

A Pre-exponential constant

Ad Droplet cross-sectional area, m2

As Droplet surface area, m2

A0 Nozzle cross sectional area. m2

Cp Specific heat, J/kg-K

Cam Reaction progress variable

C Coefficient of discharge of nozzle

Cd Reference specific heat at temperature T0

**ABBREVIATIONS**

ATDC After Top Dead Center

BDC Bottom Dead Center

BTDC Before Top Dead Center

CA Crank Angle

CAD Computer Aided Design

CCS Combined Charging System

CFD Computational Fluid Dynamics

CO Carbon Monoxide

CTC Characteristic–Time Combustion

**Abstract**

In an era where cyber threats are becoming increasingly sophisticated, ensuring a safe browsing experience is paramount. **SAFESURF** is a lightweight Chrome extension developed using **JS** and the **VIRUS-TOTAL API** to enhance online security by providing real-time monitoring and scanning of URLs and downloaded files. Unlike traditional security tools that focus solely on either URL analysis or file scanning, SAFESURF integrates both functionalities to offer **comprehensive protection against phishing, malware, and other cyber threats**.

The extension leverages **threat intelligence APIs**, including **VirusTotal** and **Google Safe Browsing**, to analyze URLs and file signatures in real time. It employs browser APIs such as **webRequest** for network request interception and **downloads** for file monitoring, ensuring that users are safeguarded against malicious content before exposure. The HTML & JS based user interface provides an intuitive dashboard where users can **view scan results, receive threat notifications, and manage security settings**, including **customizable whitelisting** of trusted URLs and blacklisting of untrusted URLs.

By combining robust backend security mechanisms with a user-friendly interface, SAFESURF aims to bridge the gap in existing browser security tools. It empowers users with **proactive threat detection, real-time alerts, and customizable security controls**, ensuring a **safer and more secure** browsing experience.

**REFERENCES**

**1**. **VirusTotal (2004).** A multi-engine scanning platform for detecting malware.

* Aggregates antivirus scans and threat intelligence from multiple vendors to analyze URLs and files for potential malware and malicious activities.

**2. Virustotal File Scanning (2004).** Cloud-based malware scanning for downloads.

* Provides a centralized file scanning service that allows users to check downloaded files against multiple antivirus engines before execution.

**3. PhishTank (2006).** A community-driven phishing database.

* Maintains a publicly accessible list of reported phishing websites, helping users and security tools detect fraudulent web pages.

**4.** **Avast Online Security (2012).** Browser extension for real-time URL threat detection.

* A security extension that warns users about potentially unsafe websites by leveraging blacklists and heuristic analysis.

**5. Malwarebytes Browser Guard (2019).** Enhancing browser security against malicious content.

* A browser extension designed to block malware, trackers, and phishing websites, but lacks file analysis features.

**6. Lippmann, R., et al. (2021).** Layered security approaches for web-based threats.

* Discusses multi-layered security strategies that combine URL scanning, sandboxing, and network monitoring for robust web protection.

**7. Z. Chen, et al. (2022).** A real-time threat detection framework for browsers. IEEE Transactions on Cybersecurity.

* Proposes a framework that integrates network traffic monitoring with browser security to detect malicious activities in real time.

**1.2 Problem Statement**

**Current security extensions lack the capability to effectively combine both URL scanning and downloaded file scanning in a unified solution.**

Many security tools today focus either on scanning URLs or on scanning downloaded files, but they typically do not integrate both functions. URL scanning identifies potentially dangerous websites, while file scanning looks for threats in downloaded files, such as viruses or malware. However, no solution currently offers real-time, integrated scanning for both of these elements together, leaving gaps in overall protection.

**This gap in functionality leaves users vulnerable to multi-vector threats, increasing the risk of cyber attacks, data breaches, and system compromises.**

Malicious websites and downloaded files often work together to launch attacks. For example, a harmful website might lead to the download of a malicious file, which could infect the system. Tools that only scan URLs or only scan files miss the full picture. Users could be exposed to threats like drive-by downloads or exploit kits, where both website and file components play a role in the attack. This lack of integrated protection increases the risk of attacks going undetected.

**The need for an all-in-one security extension that can scan both URLs and downloaded files simultaneously is critical to enhancing user protection.**

An integrated solution that scans both URLs and files in real-time would offer more comprehensive security. Such a tool could block access to dangerous sites and also scan any downloaded files for threats.

**2. Literature Survey**

Cyber threats are evolving, with malicious websites often leading to harmful file downloads. However, most existing browser security extensions focus on either **URL scanning** or **file scanning**, leaving users vulnerable to multi-vector attacks.

Some well-known extensions include:

* **PIXM** – Uses AI to detect phishing attacks in real-time but lacks file scanning.
* **PhishDetector** – Identifies phishing websites but does not analyze downloaded files.
* **AI Phishing Assistant** – Machine learning-based phishing detection but no file scanning.
* **OPSWAT File Security** – Scans downloaded files for malware but does not monitor URLs.

### **Need for SAFESURF**

To address this gap, **SAFESURF** integrates **both URL and file scanning** in a single browser extension. It uses **VirusTotal API** to protect users in real-time. The extension provides **instant alerts, customizable whitelisting, and seamless protection** against phishing, malware, and other cyber threats, ensuring a safer browsing experience.

**2.1 Existing Work**

Various browser security extensions have been developed to protect users from cyber threats, primarily focusing on **either URL scanning or file scanning**. Extensions like **PIXM, PhishDetector, and AI Phishing Assistant** specialize in identifying phishing attempts by analyzing website content and flagging suspicious URLs. On the other hand, tools such as **OPSWAT File Security for Chrome** focus on **scanning downloaded files** for malware, ensuring that harmful files are detected before they are executed. Additionally, services like **Google Safe Browsing and VirusTotal** provide real-time threat intelligence, allowing developers to integrate blacklist-based protection against unsafe websites and malicious files. While these tools are effective in their respective domains, they operate **independently**, lacking a comprehensive approach that integrates both web and file security within a single, seamless solution.

**2.2 Limitations of Existing Work**

Despite the availability of these security tools, existing browser extensions have several limitations that leave users vulnerable to modern cyber threats. The primary drawback is that most security extensions focus on **either URL scanning or file scanning**, failing to provide a **unified, real-time protection mechanism**. Malicious websites often lead to harmful file downloads, but without an integrated security approach, users remain exposed to **multi-stage cyberattacks** such as drive-by downloads and phishing-based malware infections.

Moreover, many of these tools rely heavily on **static blacklists**, which can quickly become outdated as cybercriminals continuously generate new phishing domains and malware variants. This limits their effectiveness against **zero-day threats** and newly emerging attack techniques. Additionally, some security extensions require **manual scanning** instead of offering automated, real-time protection, making them less efficient for proactive threat detection.

Another significant limitation is the **lack of user customization options**. Many existing solutions do not allow users to **whitelist trusted websites or adjust scanning settings**, which can lead to unnecessary warnings or false positives. Furthermore, some tools may introduce **performance overhead**, slowing down browsing speed due to inefficient scanning mechanisms.

Given these challenges, there is a need for a **comprehensive security extension** that integrates **real-time URL and file scanning**, leveraging threat intelligence APIs and AI-driven threat detection to offer **seamless, automated protection** against phishing, malware, and other web-based attacks.

**4.6 System Architecture**

