PACE Conclave 2025

ICEST 2025
INTERNATIONAL CONCLAVE ON
ENGINEERING SCIENCES & TECHNOLOGY

ARTELLIGENCE 2025
INTERNATIONAL CONFERENCE ON
ARTIFICIAL INTELLIGENCE

An Intelligent Approach to Safe and Secure Web Access

Mohammed Shafiulla,[†,‡,‡] Sravya M ,[¶] Sony A ,[¶] Shalini G ,[¶] and Sreeram Dheeraj[*,¶,‡]

[†]*Department of Computer Science of Engineering, Ballari Institute of Technology and Management, Karnataka, Ballari, India*

E-mail: sreeramdheeraj198@gmail.com

Abstract

Phishing attacks are becoming an increasing cybersecurity threat, with individuals being cheated by revealing personal and financial data through spam emails and websites. The majority of the available phishing detection tools like blacklists and rule-based filtering lag behind as far as adapting to changing attack methods are concerned. These conventional methods have the propensity to generate high false positives and miss new threats that have been discovered, subjecting users to cyber attacks.

To solve this problem, the authors introduce Safe and Secure Browsing, an AI-based phishing detection system with real-time deep learning, Natural Language Processing (NLP), and threat intelligence. Safe and Secure Browsing uses a hybrid deep learning architecture to scan multiple phishing indicators like website URLs, page content,

ISBN:97881-19905-39-3

HTML structure, and text patterns. Safe and Secure Browsing uses Convolutional Neural Networks (CNNs) and transformer-based models for improved detection of malicious websites and emails. In addition, Safe and Secure Browsing applies NLP-based sentiment and intent analysis for detection of deceptive language patterns typical in phishing.

Safe and Secure Browsing is different from other models in that it dynamically learns in real-time user feedback and new threat information and gets better and better at detecting the phishing as it trains. The author have tested Safe and Secure Browsing with widely known phishing datasets like PhishTank and APWG and actual phishing samples The outcome indicates that Safe and Secure Browsing achieves an accuracy of 98.7%, with a false positive of 1.2% and an F1-score of 0.97, significantly better than current detection techniques. In order to use safe and secure browsing in real-time, it can be integrated into web browsers, enterprise security software, and cloud security platforms.

The present work provides an active and efficient phishing detection framework, thereby guaranteeing users' online security as well as cybersecurity protection.

1 Introduction

The role of the internet has been so much integrated into daily life, enabling communication, business transactions, and the sharing of information or data. However, this increasing reliance on online services has opened the door to a surge in cybersecurity threats which include increasingly dangerous phishing activities carried out to compromise systems. The new face of phishing has aggravated itself cooperating with bad actors behind the curtains, to trick customers into revealing sensitive data- like credentials, financial data, and personal information. It is very true that despite security settings like blacklists, browser alerts, and even antivirus software, phishing is upside down in modernized attacks, rendering mainstream old-style detection approaches weak. Most of the disadvantages of legacy-style phishing detection are high false positives, dependent on fixed rules, and also not being able to detect Phishing on day one. This paper presents Safe and Secure Browsing, an AI-based deep-learning system for the detection of phishing that employs Natural Language.

Processing and real-time threat intelligence. The system captures and trains two models, based on CNNs and transformer-based architectures, on URL structure, content, and text patterns. Safe and Secure Browsing learns dynamically and, thus, continually updates its models on real-time threat intelligence and user input toward very significant improvements of correctly finding phishing and simultaneously reducing false alarms.

In benchmarking the performance of Safe and Secure Browsing, the author used Phish Tank in addition to actual samples which were also used in benchmarking other methods. The results show that Safe and Secure Browsing achieves a very high 98.7% accuracy with a 1.2% false positive rate and outperforms all tested benchmarked methods. Safe and Secure Browsing is meant to be implemented in real-time settings and can fit into platforms easily and without any difficulty.

2 OBJECTIVES

- Enhance Online Safety: The author aims to provide and improve online safety by identifying and warning users about potentially malicious websites before they interact with them.

- User-Friendly Interface: This tool provides an easy-to-use interface that allows individuals to check the safety of the website without needing technical expertise.

- Real-Time Phishing Detection: The author offers real- time phishing detection by utilizing up-to-date data sources, such as Phish Tank.

- User Education: The author educates users about the signs of phishing and provides guidance on how to avoid falling victim to such attacks.

- User Reviews and Resources: The author provide user reviews and additional applications related to websites, assisting users in making informed decisions about their browsing activities.

3 Experimental Procedure

3.1 Dataset Collection and Feature Preparation

This project includes the implementation of a machine learning model that is trained on a dataset of website URLs to effectively identify and classify phishing websites.The dataset was a mix of positive and negative samples, positive being phishing examples and negative being safesites. In order to make the data used by the model, features were extracted from the URL (length, special characters, and structure). These features were subsequently numericalised for the model to learn and interpret. Data was separated in two parts thereafter — one part for training the model, the other one for testing the model.

3.2 Machine Learning Model Training

Once the features were extracted, they trained a machine learning model to identify patterns that closely mimick those seen in phishing sites. An appropriate algorithm was selected which is good at handling the classification tasks. Once the model was trained, it was tested to determine how well it could distinguish phishing from safe websites. The model's accuracy was assessed with the standard measures. We obtained good experimental results and the model was ready to be applied in real-time detection.

3.3 Developing a Web Application

For the model to be useful to humans, a small web application was built. Users can simply input any desired website URL in this app to analyze. The input URL is put into computation and passed on learned model which can predict if the given site is completely safe or is a phishing site.

3.3.1 Input and Prediction

The user enters in the URL to the app. This input is then tokenized and fed to the model. The model then issues a result based on what it has learned during training.

3.3.2 Result Display

The result of the prediction is displayed on the screen indicating whether the website is a phishing or safe. In addition to the outcome, the app may offer advise for the user to surf safe online.

3.4 Visualization and Educational Characteristics

Visual components such as images and graphic are included to provide a more open and userfriendly application. These assist the user in better comprehending phishing threats and provide a more interactive and entertaining experience.

3.5 Testing and Validation

Once the system was developed, it was rigorously tested to ensure it functions as intended. Various tests were conducted, from verifying each functionality to how the entire application flowed and how easy it was for the end user to interact.

As shown in Fig.1. The flowchart outlines the method stream of a framework planned to analyse URLs and identify phishing attempts

1. User Opens Application :The method starts when the client opens the application .

2. User Signs Up: The client registers for the application by giving fundamental subtle elements.

3. Save User Details to Database: The framework spares the clients enlistment points of interest into its database.

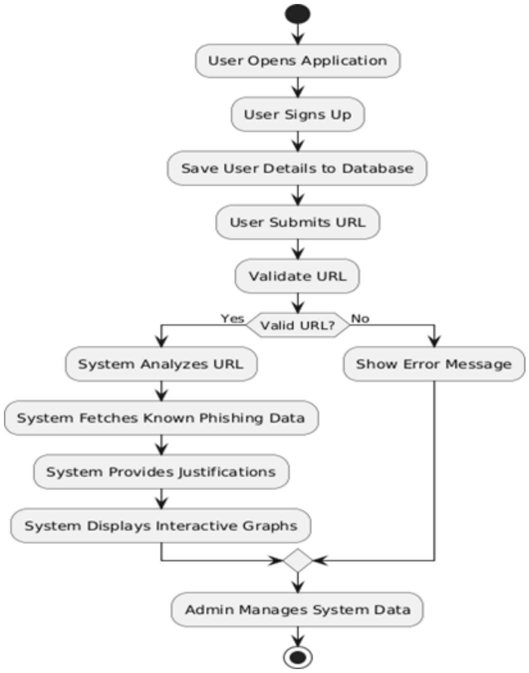

User Opens Application
User Signs Up
Save User Details to Database
User Submits URL
Validate URL
Yes
Valid URL?
No
System Analyzes URL
Show Error Message
System Fetches Known Phishing Data
System Provides Justifications
System Displays Interactive Graphs
Admin Manages System Data

Figure 1: **Flow chart workflow for URL Validation and Analysis System**

4. User Submits URL: The client gives a URL for examination.

5. Validate URL: The framework checks whether the submitted URL is substantial or not .On the off chance that the URL is invalid the framework shows an Blunder Message and stops encourage preparing. In case the URL is substantial the framework continues to the following steps.

6. System Analyzes URL:The framework starts analyzing the submitted URL for potential phishing dangers or suspicious substance.

7. System Fetches Known Phishing Data: The framework recovers information on known phishing websites to crosscheck the submitted.

8. System Provides Justifications: The framework clarifies its discoveries and reasons for hailing the URL as secure or suspicious .

9. System Displays Interactive Graphs: The framework visualizes the examination comes about utilizing intuitively charts for superior understanding.

10. Admin Manages System Data: An chairman can oversee or overhaul the frameworks data e.g. Phishing.

4 Results and Discussions

4.1 Trust Score Calculation Model

To enhance the decision-making capability of the phishing detection system, a Trust Score (TS) is computed based on various technical and user-centric indicators. The formula used is:TS = $\alpha_1 \cdot F + \alpha_2 \cdot D + \alpha_3 \cdot P + \alpha_4 \cdot U$Where:• F = SSL Certificate Validity Score (1 if valid, 0 if invalid)• D = Domain Reputation Score (range [0,1] from threat intelligence)• P = PhishTank Match Score (1 if found in database, 0 if not)• U = User Feedback Score (range [0,1])• α_1 to α_4 are weighting factors such that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$This weighted model enables dynamic scoring based on available security metrics. A higher TS indicates a safer URL, and values closer to zero suggest a potentially malicious site.

Table 1:

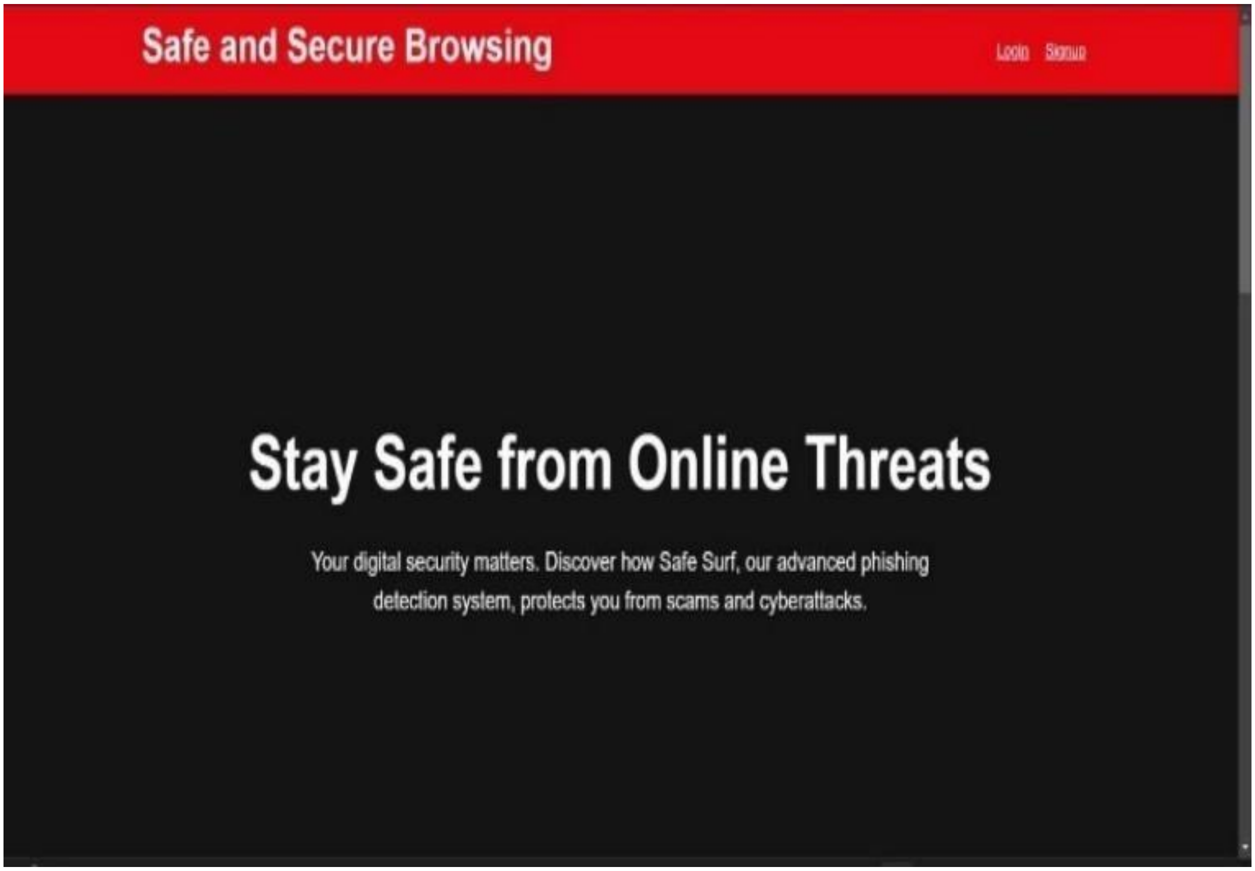
Symbol	Parameter Description	Range/Values
F	SSL Certificate Validity Score	{0, 1}
D	Domain Reputation Score	[0, 1]
P	PhishTank Match Score	{0, 1}
U	User Feedback Score	[0, 1]
α_1 to α_4	Weighting coefficients (sum = 1)	[0, 1] individually

Figure: Trust Score Formula used in Safe and Secure Browsing. The score aggregates technical and user-based indicators to evaluate the credibility of a website. Weighting factors α_1 through α_4 are calibrated based on model performance and risk assessment policies.

4.2 Sample Trust Score Calculation

To illustrate the application of the Trust Score formula, consider the following values:• F = 1 (SSL certificate is valid)• D = 0.85 (high domain reputation)• P = 0 (not found in PhishTank)• U = 0.9 (positive user feedback)• Weights: $\alpha_1 = 0.2$, $\alpha_2 = 0.3$, $\alpha_3 = 0.1$, $\alpha_4 = 0.4$Using the formula:TS = $\alpha_1 \cdot F + \alpha_2 \cdot D + \alpha_3 \cdot P + \alpha_4 \cdot U$TS = $(0.2 \times 1) + (0.3 \times 0.85) + (0.1 \times 0) + (0.4 \times 0.9)$TS = $0.2 + 0.255 + 0 + 0.36 = 0.815$Therefore, the Trust Score is

0.815, indicating that the URL is considered safe.



Safe and Secure Browsing

Stay Safe from Online Threats

Your digital security matters. Discover how Safe Surf, our advanced phishing detection system, protects you from scams and cyberattacks.

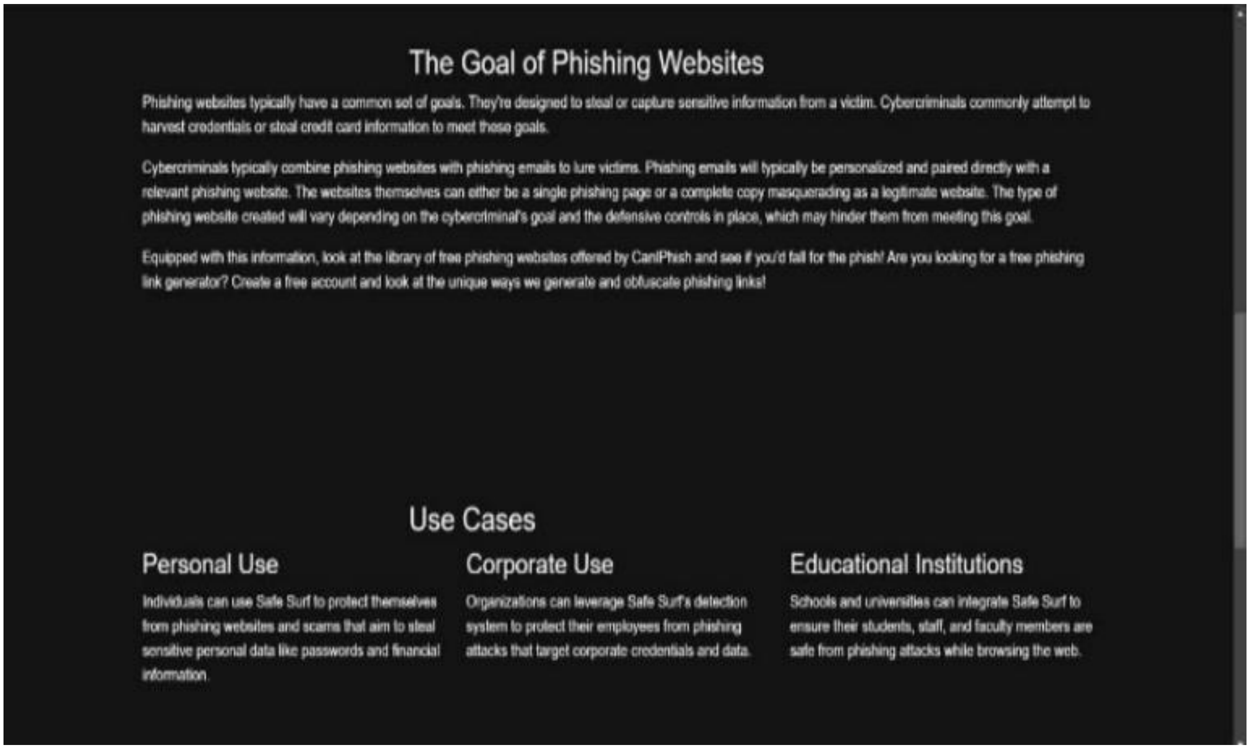
Figure 2: **2:**

As shown in the Fig2. It represents the homepage of safe and secure Browsing. Red Headline consist of project name and Login, Signup options. The main section emphasizes the protection of threats on the Internet, urging users to maintain security.

Fig5. Indicates the author can view an signup page which includes fields like email, passwords and password confirmation field.

From the above Fig6. The user enters a valid email id and password after successful Sign up of the user is completed

This Fig7. Represents the phishing detection main page which consist of a box where the URL's are checked where they are phishing or not. In the white dialog box the URL should be entered with correct format and then when clicked on green box representing 'Check URL' it processes ,analysis and represents the result.



The Goal of Phishing Websites

Phishing websites typically have a common set of goals. They're designed to steal or capture sensitive information from a victim. Cybercriminals commonly attempt to harvest credentials or steal credit card information to meet these goals.

Cybercriminals typically combine phishing websites with phishing emails to lure victims. Phishing emails will typically be personalized and paired directly with a relevant phishing website. The websites themselves can either be a single phishing page or a complete copy masquerading as a legitimate website. The type of phishing website created will vary depending on the cybercriminal's goal and the defensive controls in place, which may hinder them from meeting this goal.

Equipped with this information, look at the library of free phishing websites offered by CanIPhish and see if you'd fall for the phish! Are you looking for a free phishing link generator? Create a free account and look at the unique ways we generate and obfuscate phishing links!

Use Cases

Personal Use

Individuals can use Safe Surf to protect themselves from phishing websites and scams that aim to steal sensitive personal data like passwords and financial information.

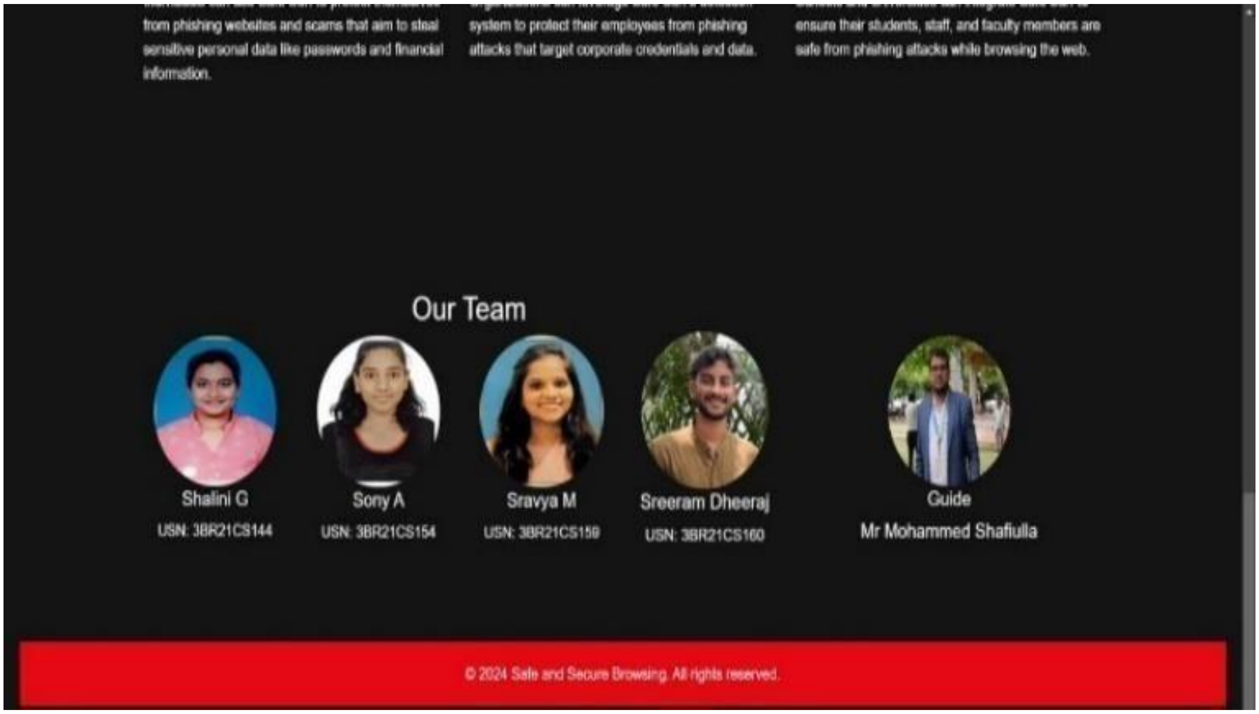
Corporate Use

Organizations can leverage Safe Surf's detection system to protect their employees from phishing attacks that target corporate credentials and data.

Educational Institutions

Schools and universities can integrate Safe Surf to ensure their students, staff, and faculty members are safe from phishing attacks while browsing the web.

Figure 3: **g 3: Goals and Use Cases of Phishing Websites**



from phishing websites and scams that aim to steal sensitive personal data like passwords and financial information.

system to protect their employees from phishing attacks that target corporate credentials and data.

ensure their students, staff, and faculty members are safe from phishing attacks while browsing the web.

Our Team

Shalini G
USN: 3BR21CS144

Sony A
USN: 3BR21CS154

Sravya M
USN: 3BR21CS159

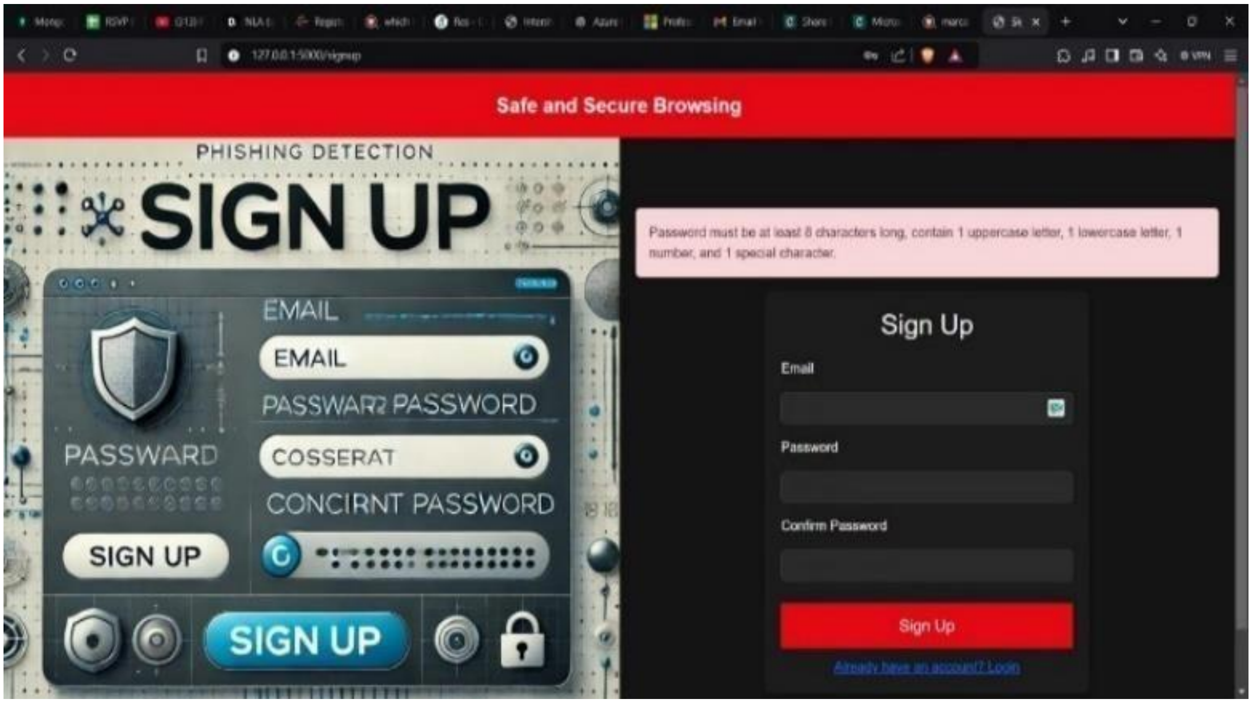
Sreeram Dheeraj
USN: 3BR21CS160

Guide
Mr Mohammed Shafiulla

© 2024 Safe and Secure Browsing. All rights reserved.

Figure 4: **4:**

ISBN:97881-19905-39-3



Password must be at least 8 characters long, contain 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.

Sign Up

Email

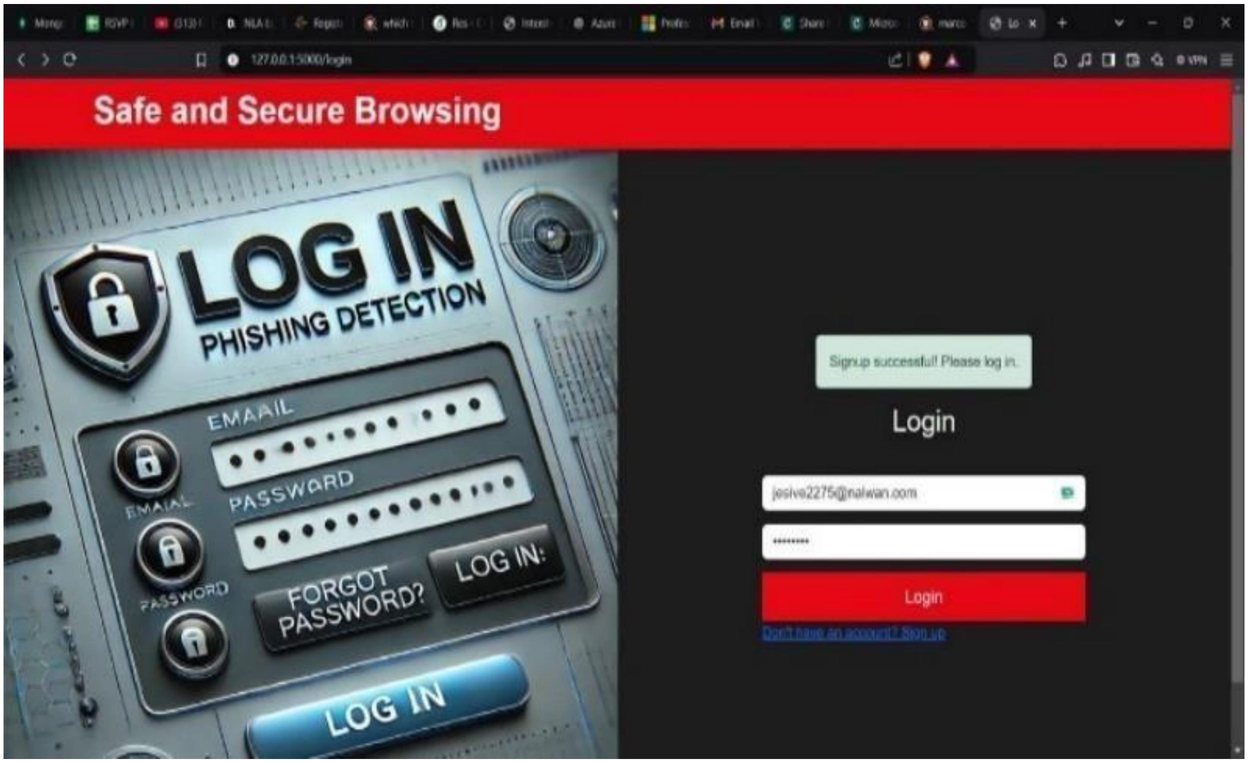
Password

Confirm Password

Sign Up

Already have an account? Login

Figure 5: **5:**



Signup successful! Please log in.

Login

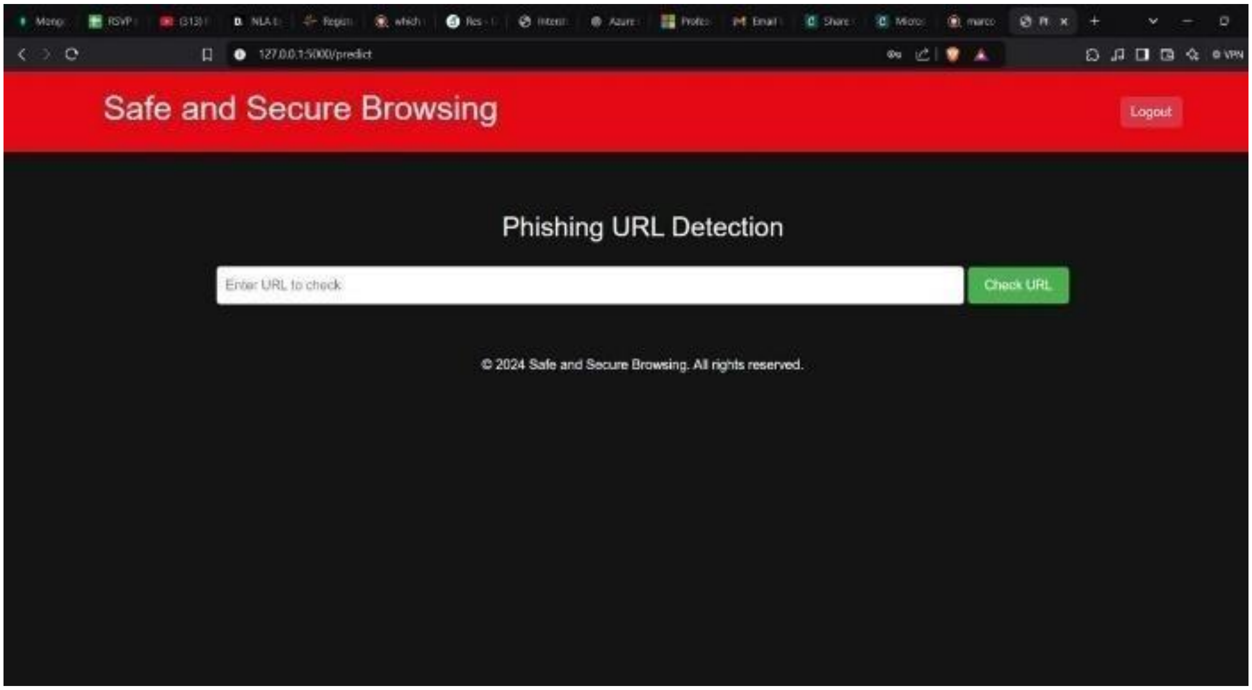
jesive2275@nalwan.com

••••••••

Login

Don't have an account? Sign up

Figure 6: **6:**

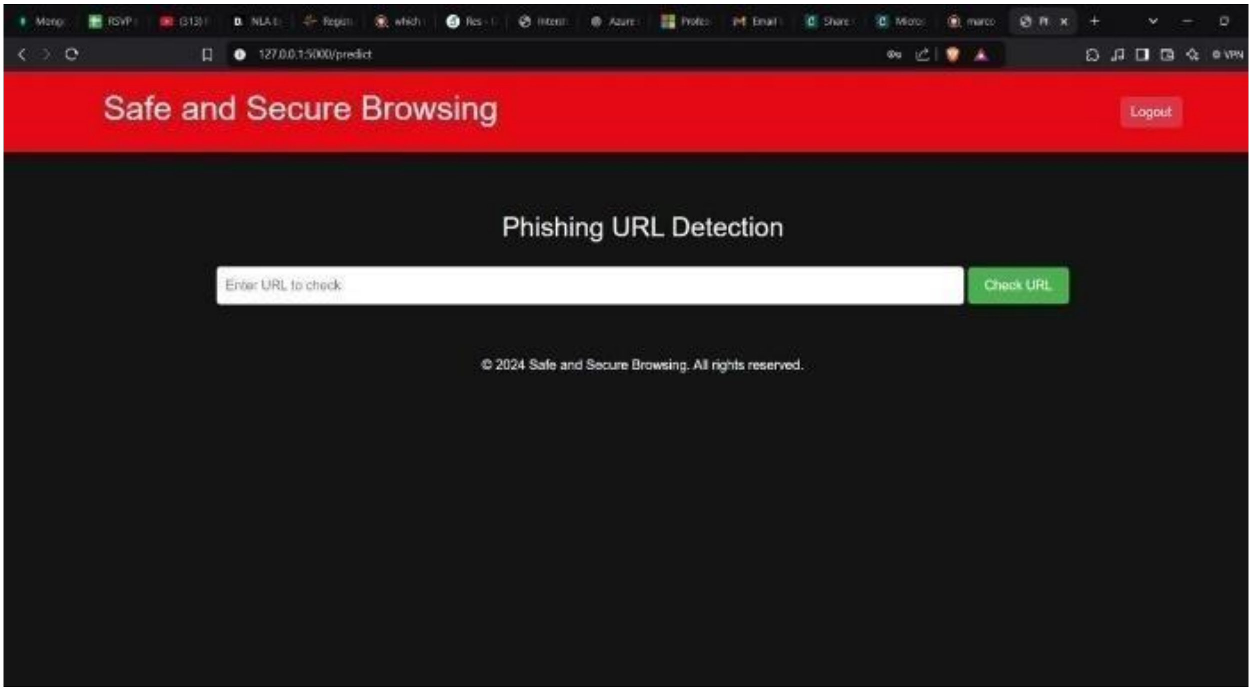


Safe and Secure Browsing

Phishing URL Detection

© 2024 Safe and Secure Browsing. All rights reserved.

Figure 7: 7:

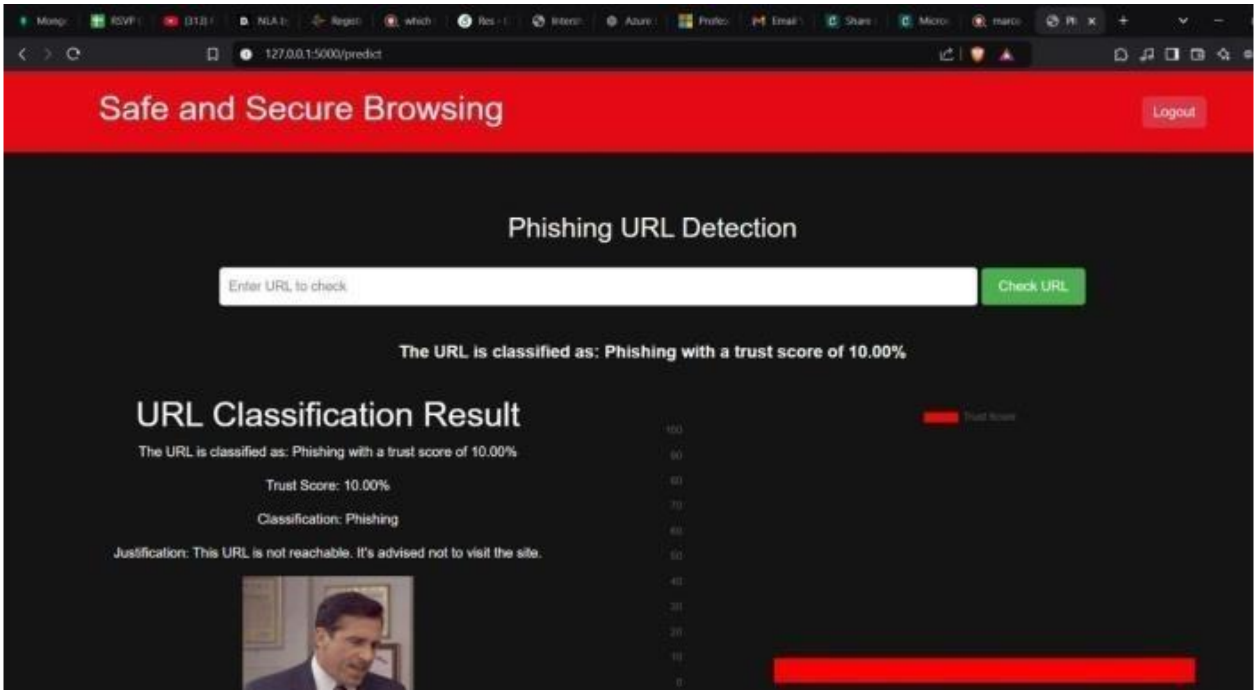


Safe and Secure Browsing

Phishing URL Detection

© 2024 Safe and Secure Browsing. All rights reserved.

Figure 8: Fig 8: Safe URL detection



127.0.0.1:5000/predict

Safe and Secure Browsing

Logout

Phishing URL Detection

Enter URL to check

Check URL

The URL is classified as: Phishing with a trust score of 10.00%

URL Classification Result

The URL is classified as: Phishing with a trust score of 10.00%

Trust Score: 10.00%

Classification: Phishing

Justification: This URL is not reachable. It's advised not to visit the site.

Figure 9: **Fig 9. Phishing URL detection**

We can understand from Fig9. That the URL which is submitted is a phishing website URL .It indicates Phishing website in red colour along with low score .It represents that the trust score is 10% and it is not a Legitimate website.

4.3 Conclusion

In this study, we proposed safe and safe browsing designed to upgrade online security safety by integrating and assessing dangers by integrating the advanced machine learning algorithm with phish tank. Through trust scores, threat alerts, and active community participation, users are allowed to make informed decisions, minimizing exposure to phishing attacks while also reducing .Future enhancements can focus on improving detection accuracy using deep learning models, expanding the system to mobile platforms and browser extensions, and integrating blockchain-based security verification for enhanced reliability. Leveraging crowdsourced threat intelligence and implementing automated incident response mechanisms will further strengthen phishing detection capabilities and to use, Safe and Secure Browsing brings out an important tool for druggies to reach safer Internet operation.

Acknowledgement: We'd like to extend our sincere gratefulness to Dr. R.N. Kulkarni, Head of the Department of Computer Science and Engineering at Ballari Institute of Technology and Management, for his expert guidance, nonstop support, and stimulant throughout this design. His precious perceptivity have greatly told the direction of our exploration and contributed significantly to the successful completion of this work.