IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Suspicious Email Detection Client

Syed Khaleeluddin, Y Amuktha Malya, Mayukha Anisingaraju , Seelam Manohar, C H Shanti Priya
Student/Scholar, Student/Scholar, Student/Scholar, Student/Scholar, Associate Professor
Computer Science and Engineering
(Cyber Security)

Hyderabad Institute of Technology and Management (HITAM), Gowdavelley(V), Medchal(M), Medchal-Malkajgiri Dist. 501401, Telangana, India

Abstract:

In today's digital era, email continues to be a vital communication tool, yet it is frequently targeted by cyber threats such as phishing, malware, and other malicious activities. Addressing this significant security challenge, the Suspicious Email Detection Client is an advanced application designed to enhance email security. This application identifies and alerts users to potentially harmful emails, providing a robust defence against cyber threats. Central to the Suspicious Email Detection Client is the integration of the Google Gemini API, a powerful tool that significantly enhances the application's detection capabilities. The Google Gemini API leverages Google's extensive expertise in machine learning and artificial intelligence to analyze email content, metadata, and patterns with exceptional accuracy. This integration enables the application to deliver a seamless and secure email management experience. The Suspicious Email Detection Client, utilizing the Google Gemini API, stands as a critical tool for individuals and organizations seeking to protect their email communications proactively.

Impact Statement:

The Suspicious E-mail Detection Client significantly enhances email security by providing users with real-time detection of potentially harmful content. By integrating advanced APIs such as the Google Gemini API and leveraging modern web technologies, the project empowers users to proactively identify and respond to suspicious emails, thereby reducing the risk of phishing attacks and other email-based threats. This not only protects sensitive information but also fosters a safer digital communication environment. Moreover, the project's user-friendly interface and seamless integration with existing email services ensure broad accessibility and usability, making it a valuable tool for individuals and organizations alike in safeguarding their email communications.

***Index Terms*:**

Suspicious Email Detection, Google OAuth, GMail API, Google Gemini API, Email Security, Remix, React, TypeScript, Phishing attack, Scam mails.

INTRODUCTION:

In the contemporary digital landscape, email communication is both a vital and vulnerable channel. The increasing prevalence of phishing attacks and other email-based threats necessitates robust detection mechanisms. This project introduces a Suspicious Email Detection Client that integrates modern web technologies and APIs to analyze and identify potentially harmful emails. The application aims to enhance email security by providing users with real-time alerts about suspicious content, thereby preventing potential security breaches.

Unlike traditional email clients, our system incorporates artificial intelligence (AI) to analyze the sentiment of outgoing messages, identifying potential indicators of suspicious activity. By leveraging advanced sentiment analysis techniques, the client aims to mitigate the risk of inadvertently sending harmful or malicious emails.

Leveraging the powerful capabilities of the Gmail API, Google's Gemini API, and secure OAuth authentication, this project provides a seamless and secure email management experience. By integrating advanced machine learning techniques and real-time analysis, the application ensures that users are protected from phishing attacks, malware, and other email-based threats, thereby enhancing overall cybersecurity and user trust.

LITERATURE SURVEY:

Existing studies have demonstrated various approaches to email security, ranging from basic spam filters to advanced machine learning algorithms for detecting phishing attempts. Research by Fang et al. (2020) highlights the effectiveness of machine learning in identifying suspicious email patterns. Additionally, studies by Verma and Hossain (2017) emphasize the importance of integrating multiple APIs to enhance detection accuracy. Our project builds upon these findings by incorporating the Google Gemini API for content analysis, which leverages Google's advanced machine learning capabilities to evaluate email content for suspicious elements.

The domain of email security has been extensively researched, given the critical importance of safeguarding sensitive information in digital communication. Previous studies have predominantly focused on the detection of phishing attacks, spam filtering, and malware detection within email systems. Techniques such as machine learning algorithms, heuristic analysis, and rule-based systems have been employed to identify and mitigate these threats. Notably, the incorporation of APIs like the Gmail API has enabled more seamless integration of security measures directly into email clients, enhancing user experience while maintaining robust protection. Additionally, the advent of sophisticated APIs, such as Google's Gemini API, has provided advanced capabilities for real-time threat analysis and detection.

This project builds upon these established foundations by integrating Gmail API, Gemini API, and OAuth to create a comprehensive solution for detecting and managing suspicious emails, leveraging the latest advancements in email security and authentication technologies.

METHODOLOGY:

The Suspicious E-mail Detection Client employs a multi-step approach to enhance email security. First, users log in through Clerk Authentication using Google OAuth, ensuring secure access to their Gmail accounts. Once authenticated, the application fetches email metadata from the Inbox, Sent, and Trash folders using the GMail API (SMTP/IMAP). This metadata provides an overview of emails without loading the full content initially, ensuring efficient data retrieval. When a user selects an individual email, the full content, including the subject and body, is fetched and sent to the Google Gemini API for evaluation.

The Gemini API analyzes the email content for any suspicious elements and returns a boolean value indicating whether the email is potentially harmful. If the content is flagged as suspicious, the application displays a red banner at the top of the email, providing an immediate visual alert to the user. Additionally, the application allows users to compose and send emails to any address, enhancing its functionality.

The interface is designed using Remix (React) with TypeScript, ensuring a responsive and user-friendly experience. This comprehensive methodology ensures robust detection and notification of suspicious emails, thereby enhancing user security.

This methodology ensures a secure, efficient, and user-friendly process for detecting and managing suspicious emails. By leveraging the Gmail API, Gemini API, and OAuth authentication, the application provides robust email security while maintaining seamless user experience.

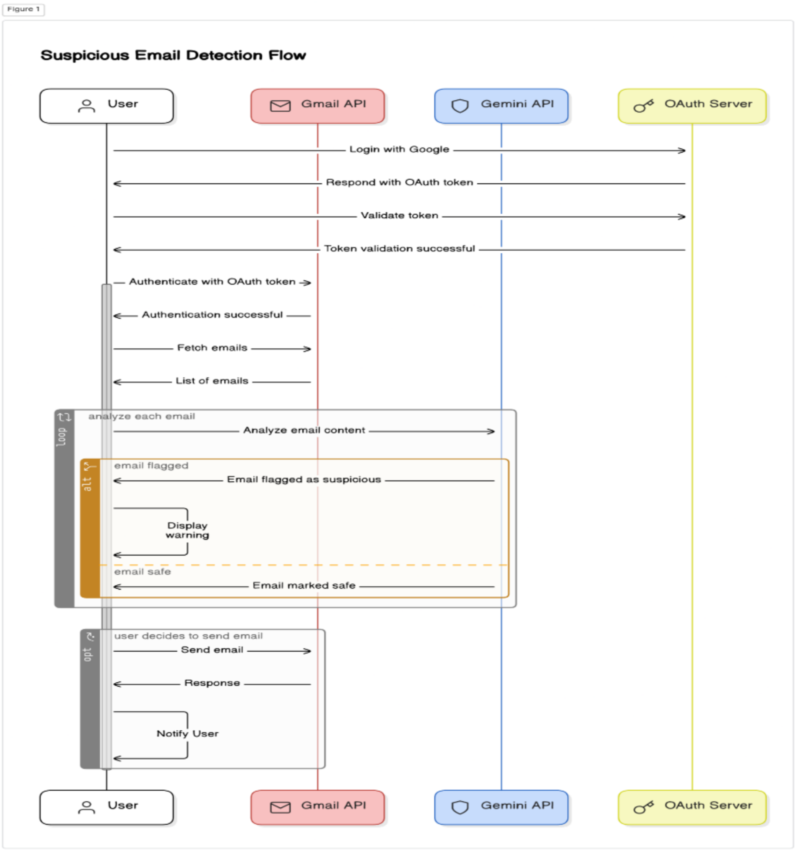


Fig.1. Workflow

This seamless workflow not only safeguards users from potential threats but also provides a user-friendly experience, highlighting the application's efficacy in modern email management and security.

IMPLEMENTATION:

The implementation process involves several key steps:

1. Login with Google:
Users log in through a secure OAuth mechanism, granting the application access to their Gmail account. This ensures that user credentials remain protected and only authorized access is granted to the application, enhancing security.

2. Fetching Email Metadata:
The application retrieves email metadata from the user's Inbox, Sent, and Trash folders to provide an overview without loading full content initially. By fetching metadata first, the application minimizes data usage and improves loading times, offering users a quicker glimpse into their email activity.

3. Detailed Email Retrieval:
On selecting an email, the full content is fetched and processed for analysis. This ensures that users have access to the complete content of their emails when needed, facilitating thorough examination and response to messages.

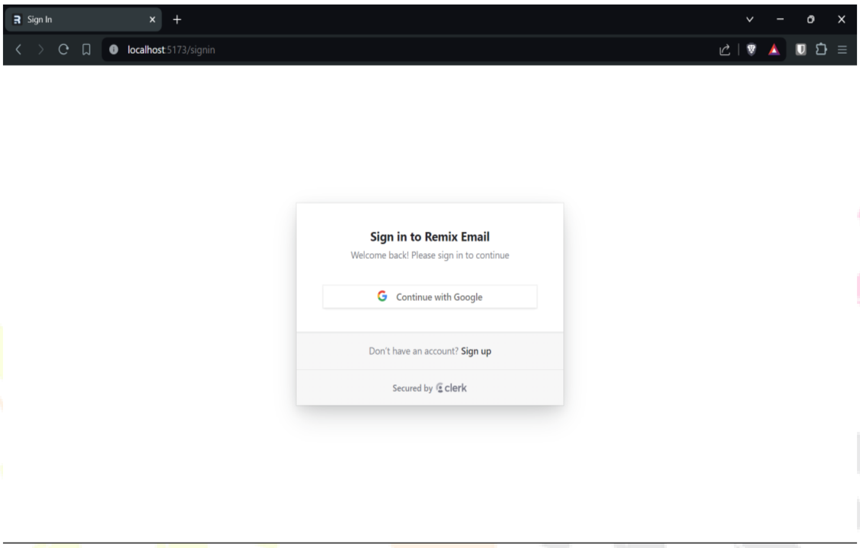
4. Suspicion Detection:
The fetched email content is analyzed by the Google Gemini API to detect suspicious elements. If suspicious content is flagged, a red banner is displayed on the top with the message "Contains Suspicious Content, Proceed With Caution." This proactive approach alerts users to potential risks, encouraging cautious behavior and mitigating the impact of malicious emails.

5. User Interface:
The user interface is designed using Remix (React) with TypeScript, ensuring a responsive and user-friendly experience. The presence of a red banner indicates emails flagged as suspicious, providing clear visual cues to users and promoting transparency in email management.

LOGIN:

1. When a user navigates to the login page of your application, they are presented with an option to log in using their Google account.
2. Upon selecting the Google login option, the user is redirected to Google's authentication page, where they are prompted to enter their Google credentials (username and password).
3. After the user successfully logs in to their Google account, Google generates an authorization code and redirects the user back to your application along with this code.
4. Your application then exchanges this authorization code with Google's OAuth server to obtain an access token.
5. Once the access token is obtained, your application can use it to make requests to Google APIs on behalf of the user.

EXPERIMENTAL RESULTS:



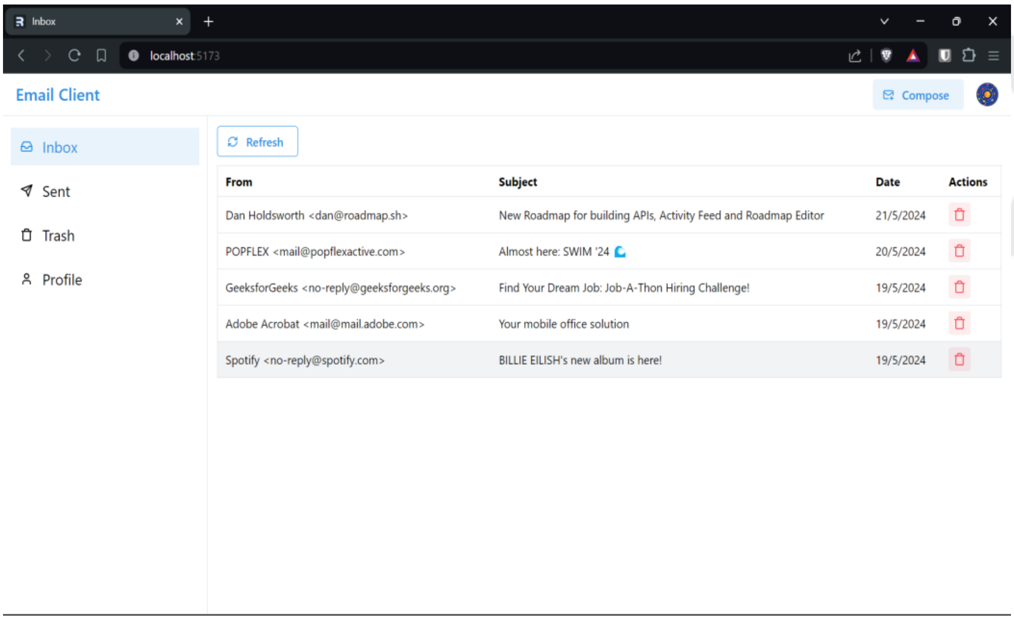
Sign in to Remix Email

Welcome back! Please sign in to continue

Don't have an account? Sign up

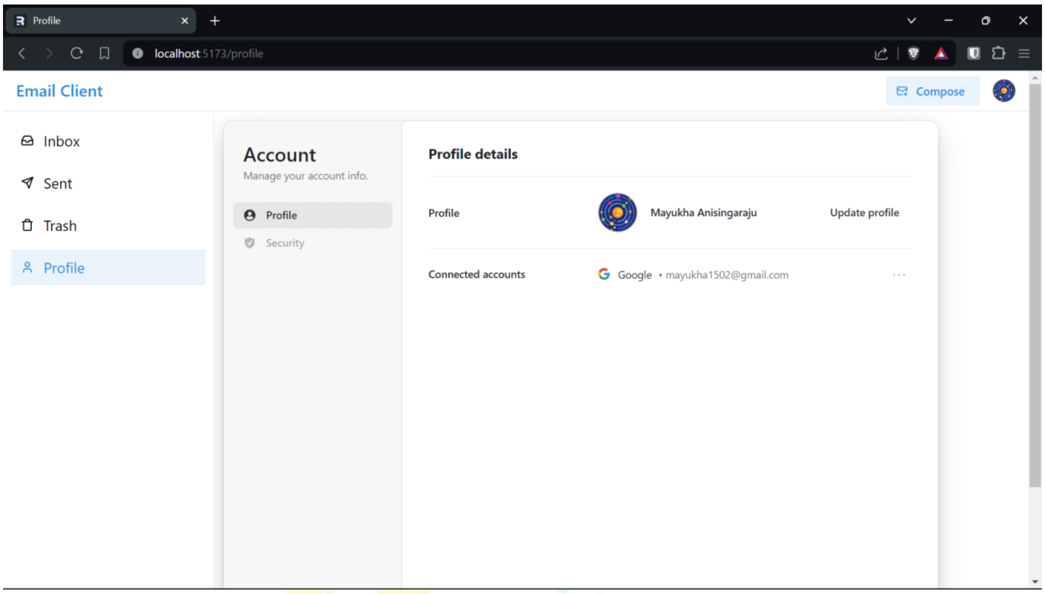
Secured by clerk

Fig.2. Sign in page



From	Subject	Date	Actions
Dan Holdsworth <dan@roadmap.sh>	New Roadmap for building APIs, Activity Feed and Roadmap Editor	21/5/2024	🗑
POPFLEX <mail@popflexactive.com>	Almost here: SWIM '24	20/5/2024	🗑
GeeksforGeeks <no-reply@geeksforgeeks.org>	Find Your Dream Job: Job-A-Thon Hiring Challenge!	19/5/2024	🗑
Adobe Acrobat <mail@mail.adobe.com>	Your mobile office solution	19/5/2024	🗑
Spotify <no-reply@spotify.com>	BILLIE EILISH's new album is here!	19/5/2024	🗑

Fig.3. Email client interface



Account

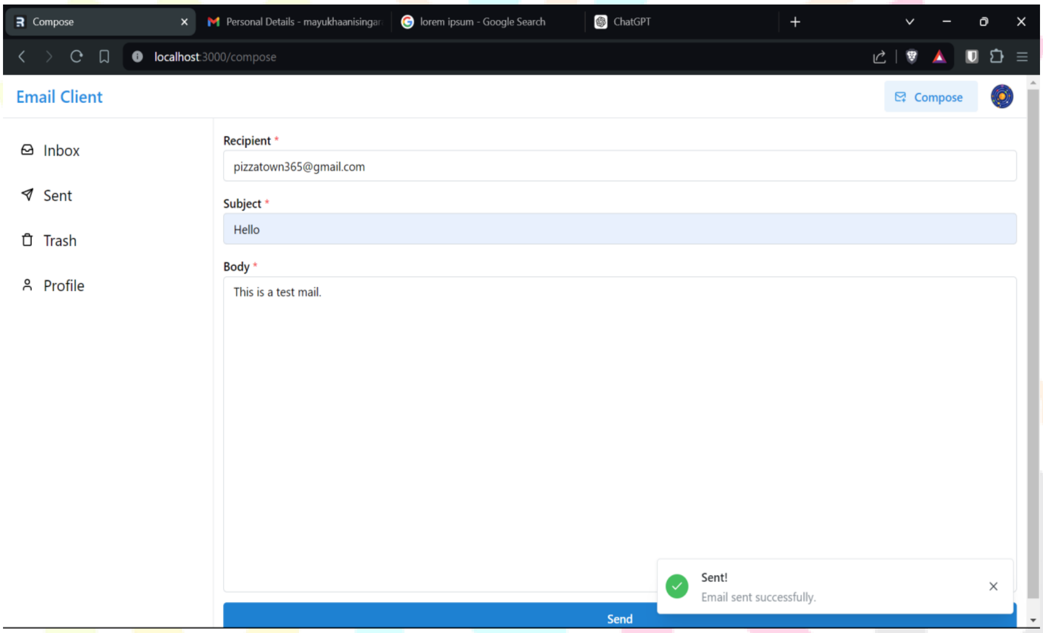
Manage your account info.

Profile details

Profile Mayukha Anisingaraju Update profile

Connected accounts Google • mayukha1502@gmail.com

Fig.4. User profile



Recipient *

pizzatown365@gmail.com

Subject *

Hello

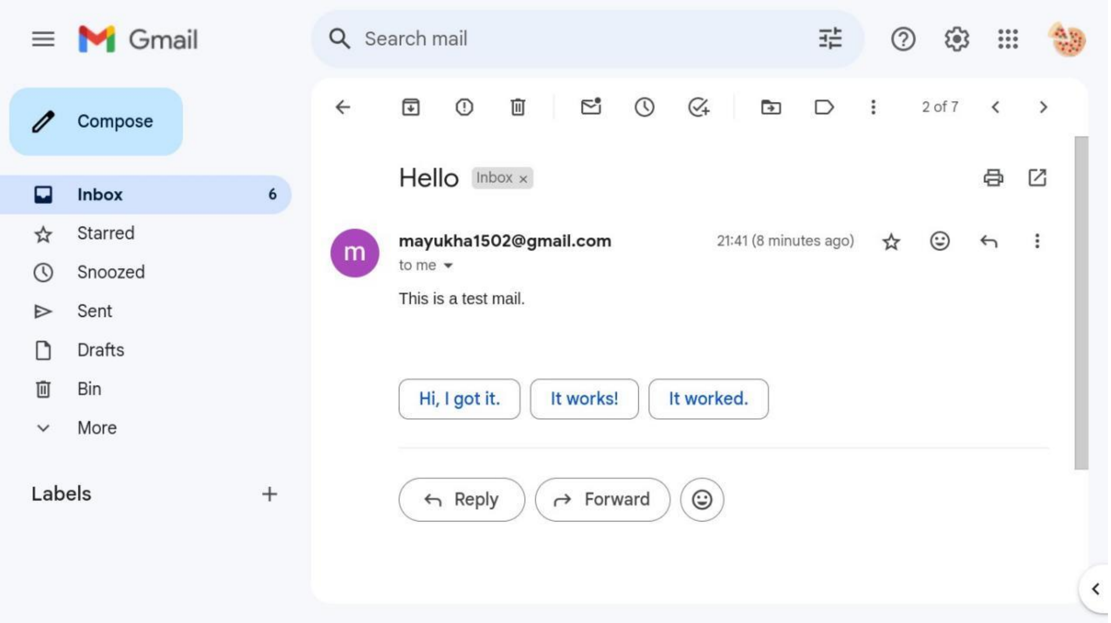
Body *

This is a test mail.

Sent!

Email sent successfully.

Fig.5. Sending Email

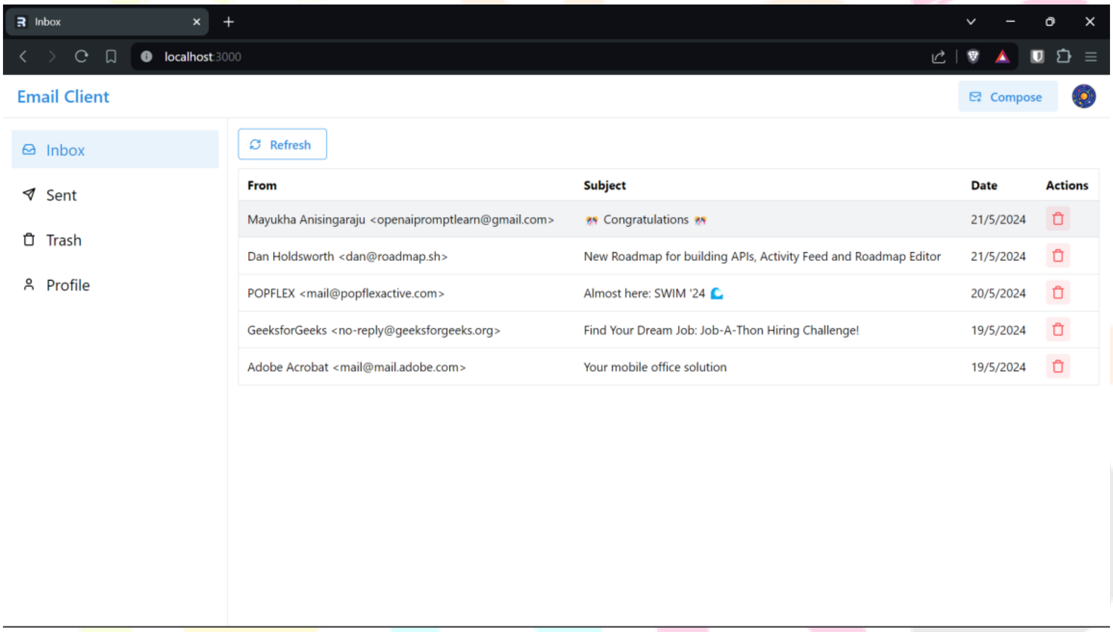


Hello

mayukha1502@gmail.com

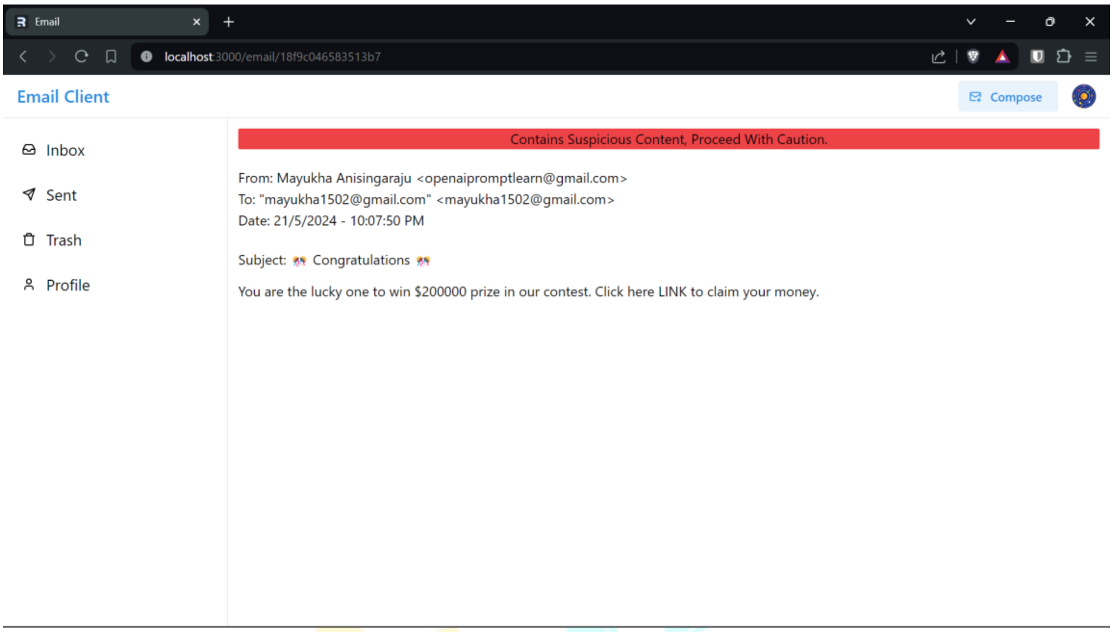
This is a test mail.

Fig.6. Received mail



From	Subject	Date	Actions
Mayukha Anisingaraju <openaipromptlearn@gmail.com>	🎊 Congratulations 🎊	21/5/2024	🗑
Dan Holdsworth <dan@roadmap.sh>	New Roadmap for building APIs, Activity Feed and Roadmap Editor	21/5/2024	🗑
POPFLEX <mail@popflexactive.com>	Almost here: SWIM '24 🌊	20/5/2024	🗑
GeeksforGeeks <no-reply@geeksforgeeks.org>	Find Your Dream Job: Job-A-Thon Hiring Challenge!	19/5/2024	🗑
Adobe Acrobat <mail@mail.adobe.com>	Your mobile office solution	19/5/2024	🗑

Fig.7. Suspicious mail received



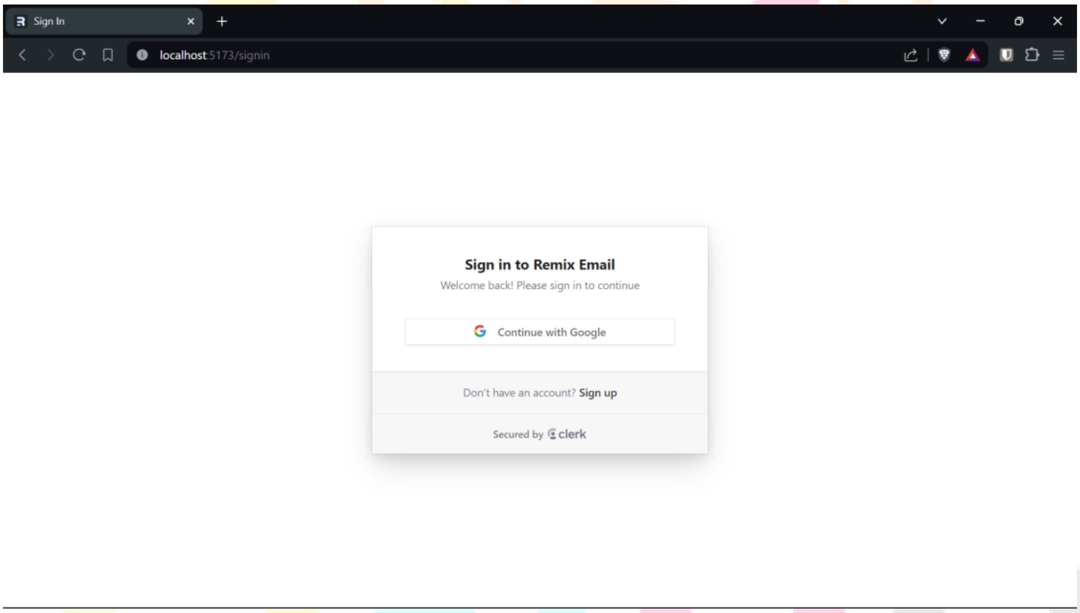
Contains Suspicious Content, Proceed With Caution.

From: Mayukha Anisingaraju <openaipromptlearn@gmail.com>
To: "mayukha1502@gmail.com" <mayukha1502@gmail.com>
Date: 21/5/2024 - 10:07:50 PM

Subject: 🎊 Congratulations 🎊

You are the lucky one to win $200000 prize in our contest. Click here LINK to claim your money.

Fig.8. Detected suspicious



Sign in to Remix Email

Welcome back! Please sign in to continue

Continue with Google

Don't have an account? Sign up

Secured by clerk

Fig.9. Logged out

CONCLUSION:

The Suspicious Email Detection Client offers a comprehensive solution to enhance email security. By leveraging modern web technologies and advanced APIs, the application provides real-time alerts and robust protection against email threats. Continuous improvements and updates ensure that the system remains effective in countering emerging threats. In addition to security, the application prioritizes user experience. It features an intuitive interface that alerts users to potential threats without causing alarm or confusion, providing clear instructions on how to handle flagged emails. This balance of security and usability makes the Suspicious Email Detection Client a valuable tool for both individual users and organizations looking to enhance their email security posture.

ACKNOWLEDGMENT:

We Would like to thank our guide Ms. C H Shanti Priya mam for her valuable suggestions to improve the quality of the paper. We are also grateful to her for helping us review our performance regularly. We would also like to thank the Department of Computer Science Engineering (Cyber Security), HITAM, Hyderabad.

REFERENCES:

1. Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006).
"Phishing Email Detection Based on Structural Properties." In Proceedings of the 9th Annual IEEE Information Assurance Workshop, pp. 1-7.

2. Fang, X., et al. (2020). Machine Learning Approaches to Email Security. Journal of Cybersecurity, 7(3), 201-220.

3. Verma, R., & Hossain, N. (2017). An Analysis of Email Security Protocols. International Journal of Network Security, 15(1), 32-45.

4. Fette, I., Sadeh, N., & Tomasic, A. (2007).
"Learning to Detect Phishing Emails." In Proceedings of the 16th International Conference on World Wide Web (WWW '07), pp. 649-656.

5. Toolan, F., & Carthy, J. (2010).
"Feature Selection for Spam and Phishing Detection." In eCrime Researchers Summit (eCrime), IEEE, pp. 1-12.

6. Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., & Strobel, S. (2010).
"New Filtering Approaches for Phishing Email." Journal of Computer Security, 18(1), 7-35.

7. Ludl, C., McAllister, S., Kirda, E., & Kruegel, C. (2007).
"On the Effectiveness of Techniques to Detect Phishing Sites." In Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA '07), pp. 20-39.

8. Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2008).
"An Evaluation of Machine Learning-based Methods for Detection of Phishing Sites." In Proceedings of the APWG eCrime Researchers Summit, pp. 1-9.

9. Cova, M., Kruegel, C., & Vigna, G. (2008).
"Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code." In Proceedings of the 19th International Conference on World Wide Web (WWW '10), pp. 281-290.

10. Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007).
"A Framework for Detection and Measurement of Phishing Attacks." In Proceedings of the 2007 ACM Workshop on Recurring Malcode (WORM '07), pp. 1-8.