CyberPeace editor@cyberpeace.net

THE CYBERPEACE JOURNAL

Supported by United Service Institution of India

Academic Partner Shah & Anchor Kutchhi Engineering College

Robust AI Driven Phishing Detection Tool

Vishaal Yadav
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
vishaal.17444@sakec.ac.in

Pratham Rane
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
pratham.17083@sakec.ac.in

Krish Shah
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
krish.16985@sakec.ac.in

Sahil Solse
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
sahil.17243@sakec.ac.in

Prajakta Pote
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
prajakta.pote@sakec.ac.in

***Abstract*— This paper presents the design and implementation of Robust AI-Driven Phishing Detection Tool, a cutting-edge solution for real-time identification of potentially harmful URLs. Through a Chrome extension, the system continuously monitors users' browsing activities, analyzing URLs for signs of phishing and issuing immediate pop-up alerts when suspicious activity is detected. Powered by javascript-based algorithms trained on extensive datasets, the system's detection capabilities evolve dynamically to stay ahead of emerging threats. Furthermore, a centralized data management system securely stores detection outcomes, facilitating comprehensive trend analysis and security insights. Complemented by an intuitive Android app, users gain clear visualizations of their browsing activity and phishing detection trends, ensuring robust protection against online threats.**

Keywords—* Phishing Detection, AI Driven, chrome extension, Mobile Application, Real-time Monitoring.

I. Introduction

Our solution is an advanced AI-driven phishing detection system designed to identify potentially harmful URLs in real-time. Through a Chrome extension, we continuously monitor the websites users visit, analyzing their URLs for signs of phishing. The extension provides immediate pop-up alerts when it detects suspicious activity, allowing users to quickly make informed decisions about their online safety. This real-time monitoring is powered by javascript based algorithms that learn from vast data sets, ensuring that our detection capabilities are constantly evolving to stay ahead of emerging threats. Beyond immediate detection, our solution offers a centralized data management system where detection outcomes are stored securely. This database links each record with the user's ID, prediction result, and timestamp, enabling comprehensive trend analysis and security insights. To complement the browser extension, we offer an Android app that provides users with a clear visualization of their browsing activity, including graphical representations of phishing detection trends. Through this combination of real-time detection, secure data storage, and user-friendly mobile app integration, our solution provides robust protection against phishing threats.

II. Literature Review

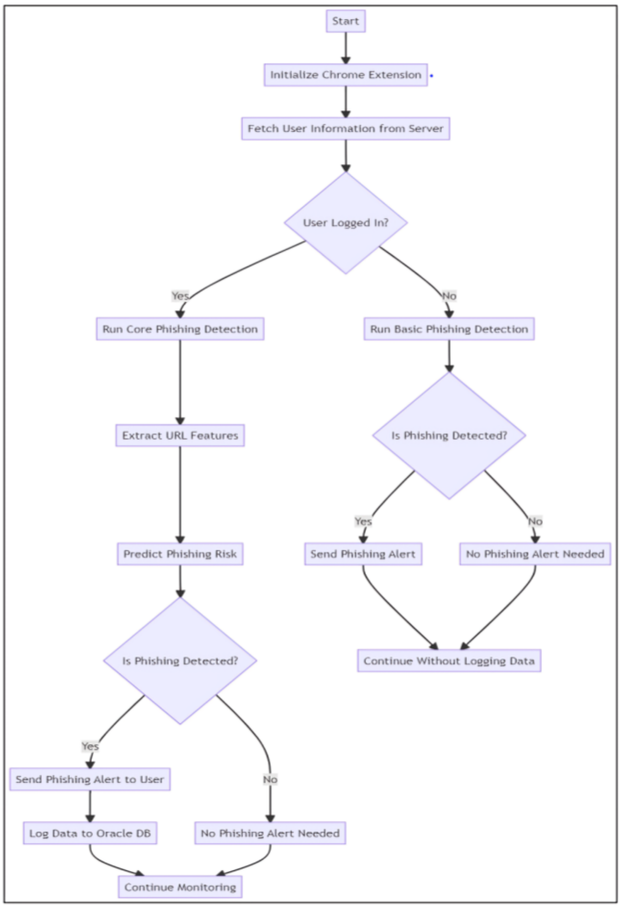
Various researchers have proposed novel approaches to combat phishing attacks, a prevalent online deception tactic causing financial losses and security breaches. **Jain, Gupta et al.** (2016) [3] introduced a client-side protection method using an auto-updated whitelist, addressing limitations of blacklist-based solutions and visual similarity approaches. **Prakash, Kumar et al.** (2010) [4] developed Phish Net, utilizing heuristics and an approximate matching algorithm to detect phishing URLs in real-time, achieving low false positive and negative rates. **Goel, Jain et al.** (2018) [5] focused on mobile phishing, discussing attack techniques, defenses, and challenges, providing a taxonomy of attacks and proposed solutions. **Dou, Khalil, Khreishah et al.** (2017) [6] conducted a systematic study of phishing detection methods, highlighting the diversity in approaches and evaluation criteria. **Sheng, Wardman, Warner et al.** (2009) [7] evaluated phishing blacklists, emphasizing the importance of heuristics in addition to blacklists for effective detection. **Rao, Pais et al.** (2019) [8] introduced a visual similarity-based approach, outperforming traditional methods with high accuracy. **Jain, Gupta et al.** (2019) [9] introduced a client-side phishing detection method based on JavaScript logic, analyzing hyperlink features in website HTML. Their approach, utilizing 12 groups of specific hyperlink features, achieved over 98.4% accuracy with logistic regression, eliminating the need for third-party services and language-independence for any textual language.**Aahas, Tariff et al.** (2023) [10] studied the impact of cybercrime on e-banking adoption, finding negative effects due to hacking, identity theft, and phishing. **Jain, Richaraya et al.** (2011) [11] proposed a web browser with phishing detection techniques, demonstrating effectiveness in detecting phishing attacks. **Yue, Wang et al.** (2008) [12] introduced a deceptive bait approach, injecting false credentials into phishing websites to mitigate attacks. **Rajesh Kumar, Vinod Kumar et al.** (2015) [13] presented a method using Intelligent-Based Classification for phishing detection, surpassing previous approaches. These diverse strategies contribute to the ongoing effort to combat phishing and enhance cybersecurity in an evolving digital landscape.

III. Methodology

The project aims to develop an AI-driven tool for real-time phishing detection, providing immediate alerts to users while browsing the internet to mitigate the risk of phishing attacks and safeguard sensitive information. The Chrome extension employs various features extracted from URLs and webpage content to detect phishing attempts, utilizing a prediction algorithm based on weighted features for classification. Upon detection, users receive pop-up alerts, and data, including the URL and user ID, is sent to a Node.js server for storage and further analysis in an Oracle Database.

The server facilitates communication with the Chrome extension and an Android app, which serves as a mobile interface for user management and interaction with the backend server. Communication among the components involves the exchange of data flows, including phishing detection results and user information.

Error handling mechanisms are implemented at various stages to ensure system robustness, addressing potential issues with phishing detection, backend processing, and database interactions. Overall, the methodology integrates phishing detection, backend communication, data handling, error handling, and Android app integration to provide a comprehensive solution for detecting phishing risks and enhancing user safety while collecting data for continuous analysis and improvement.



IV. Using the Template

The project aims to develop a robust tool for phishing detection and prevention, with a focus on employing the Agile methodology for its iterative and collaborative approach. Agile's flexibility and adaptability will be crucial in navigating evolving requirements and challenges effectively. It will foster frequent communication, short development cycles, and continuous testing to ensure the project's success.

To manage the project's complexity, well-defined milestones will be established to guide the implementation process. These milestones include data collection and preparation, where a diverse dataset of phishing and legitimate URLs will be collected, preprocessed, and cleansed to remove inconsistencies. The Chrome extension development phase will focus on designing an intuitive user interface for seamless integration into the browser. The extension will process URLs in real-time, providing instant feedback to users while ensuring lightweight design to minimize resource consumption.
Integration with Kavach - The Shield, will be a critical component of the project, with meticulous attention to detail. A robust and secure API will be designed for communication between the extension and Kavach, facilitating real-time data synchronization for continuous threat updates.

Regarding the real-time images and GUI, the extension will prompt users for login upon loading, storing data in the Oracle server if logged in, and prompting new users for registration. The Node.js server will assist in appending data into the database, where login credentials and phishing predictions will be stored along with the username and visited URLs.

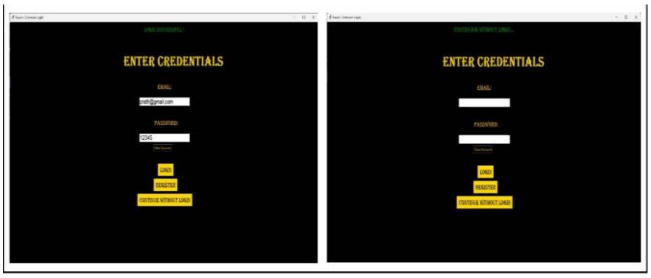
Ongoing monitoring and maintenance will be essential for the tool's continued effectiveness. This includes regular threat database updates to incorporate new phishing patterns and malicious URLs, as well as performance monitoring to address any deviations promptly.

Scalability is integral to the project's design, with cloud-based infrastructure facilitating seamless scalability as the user base grows. The project will also be flexible to accommodate future enhancements, such as additional threat detection capabilities or support for more platforms.

In conclusion, the project's approach encompasses Agile methodology, well-defined milestones, robust integration with Kavach, intuitive user interface design, ongoing monitoring and maintenance, and scalability for future enhancements, all aimed at developing an effective phishing detection and prevention tool.

V. RESULT

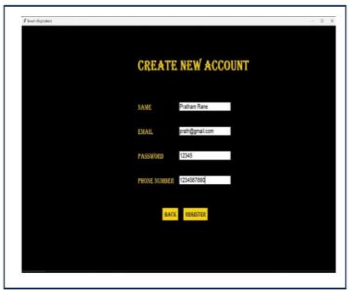
As the extension is loaded the first thing it will ask you for login.you can either login or continue without login. Also for new users it will ask them to register. After logging, you can surf through the browser and the extension will do the work properly. If the user has logged in the Data will be stored in the Oracle server else it will not be saved. The Node.js Server helps to append the data into the database. In the database the login Credentials and the phishing prediction is stored along with the username and visited URL.



EMAIL: prath@gmail.com

PASSWORD: 12345

Figure 4.1 Login Window



NAME Pratham Rane

EMAIL prath@gmail.com

PASSWORD 12345

PHONE NUMBER 1234567890

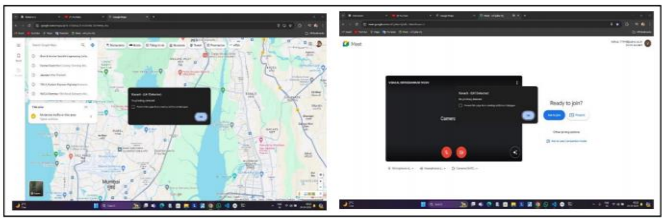


Figure 4.3 No Phishing detected Prediction

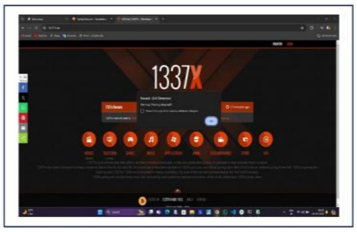
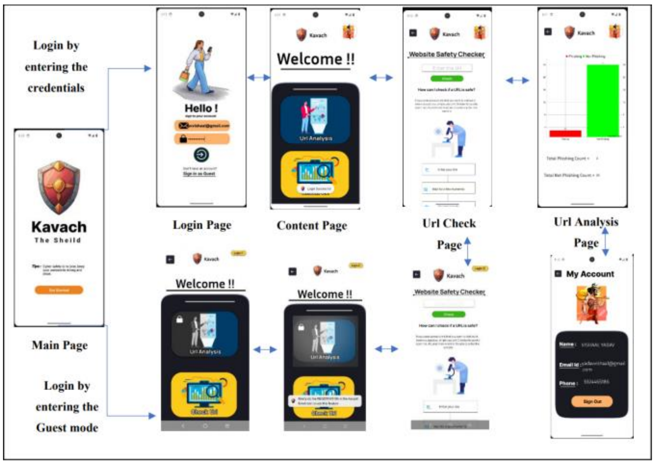


Figure 4.4 Phishing detected Prediction



VI. CONCLUSION

The AI-driven phishing detection system in this project combines a Chrome extension for real-time monitoring, an Node.js backend for data management, an Oracle Database for persistent storage, and an Android app for user interaction, creating a robust and comprehensive framework to combat phishing threats. The Chrome extension continuously analyzes URLs using feature extraction algorithms to detect phishing attempts, alerting users to potential risks. The Node.js backend serves as a central hub, processing and storing data in an Oracle Database, and also supports additional functionalities like Python script execution. The Android app, designed in Figma and developed with Android Studio, extends the system's reach to mobile users, allowing them to manage accounts and access phishing-related data on the go. Together, these components form an integrated approach that not only provides real-time protection but also facilitates secure data storage and multi-platform user engagement, offering a comprehensive solution to the growing problem of online phishing threats. Future scope includes integrating machine learning for adaptive threat detection and expanding support to additional browsers and platforms. Incorporating user behavior analysis can further enhance detection accuracy by identifying suspicious patterns.

References

[1] Alkhalil Z, Hewage C, Nawaf L and Khan I Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Front. Comput. Sci. 3:563060. doi:10.3389/fcomp.2021.563060, 2021.

[2] Tosin Ige et al,"Deep Learning-Based Speech and Vision Synthesis to Improve Phishing Attack Detection through a Multi-layer Adaptive Framework,"link.springer.com/article/10.1007/s11235-020-00733-2

[3] Jain, A.K., Gupta, B.B. et al, " Fighting against phishing attacks: state of the art and future challenges", Springer Access DOI: https://doi.org/10.1007/s00521-016-2275-y, 2016.

[4] Prakash, Manish Kumar et al," PhishNet: Predictive Blacklisting to Detect Phishing Attacks"IEEE Access,DOI: https://doi.org/10.1109/INFCOM.2010.5462216, 2010.

[5] Diksha Goel, Ankit Kumar Jain et al," Mobile phishing attacks and defense mechanisms: State of art and open research challenges",ScienceDirect Access,DOI:https://doi.org/10.1016/j.cose.2017.12.006, 2018.

[6] Dou, Z., Khalil, I., Khreishah, et al," Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection",IEEE Access,DOI: https://doi.org/10.1109/COMST.2017.2752087, 2017.

[7] Sheng, S., Wardman, B., Warner et al," An Empirical Analysis of Phishing Blacklists",FigShare Access,DOI: https://doi.org/10.1184/R1%2F6469805.V1, 2009.

[8] Rao, 4.S., Pais, A.R et al," Two level filtering mechanism to detect phishing sites using lightweight visual similarity approach",Springer Access,DOI:https://link.springer.com/article/10.1007/s12652-019-01637-z, 2019.

[9] Jain,5A.K., Gupta, B.B et al," A machine learning based approach for phishing detection using hyperlinks information",ResearchGate Access , DOI: https://link.springer.com/article/10.1007/s12652-018-0798-z, 2015.

[10] Anchal Jain and Vineet Richaraya et al," Implementing a Web Browser with Phishing Detection Techniques",Cornell University Access,DOI:https://doi.org/10.48550/arXiv.1110.0360, 2011.

[11] Chuan Yue and Haining Wang et al," Anti-Phishing in Offense and Defense", ResearchGate Access, DOI: https://doi.org/10.1109/ACSAC.2008.32, 2010.

[12] NV Rajesh Kumar and S. Vinod Kumar et al, "An effective method of phishing detection using IBC", ResearchGateAccess,DOI:https://www.researchgate.net/publication/283101545_An_effective_method_of_phishing_detection_using_IBC, 2015.

[13] Sudhanshu Gautam, Kritika Rani & Bansidhar Joshi et al, ,"Detecting Phishing Websites Using Rule-Based Classification Algorithm: A Comparison",ResearchGate Access, DOI: http://dx.doi.org/10.1007/978-981-10-3932-4_3, 2018.

[14] Ferhat Ozgur Catak,Volkan Dortkardes,Kevser Şahinbaş "Malicious URL Detection and Classification Analysis using Machine Learning",ResearchGate Access,DOI: https://doi.org/10.4018/978-1-7998-5101-1.ch008, 2020.