Machine Learning-Driven Phishing Detection: A Robust Browser Extension Solution

Sunil Kumar B.[1]; Aditya Kiran[2]; Varun E.[3]; Raghavendra D. Hegde[4]; Dev Vijay Fuletra[5]; Kunal Ittigi[6]

[1]Assistant Professor; [2,4,5,6]UG Student; [3]Associate Professor;

[1,2,3,4,5,6]Department of CSE Sai Vidya Institute of Technology Bengaluru, India

Publication Date: 2025/03/26

Abstract: This paper addresses the evolving challenge of phishing threats with the rise of sophisticated evasion techniques. The research focuses on leveraging machine learning (ML) techniques for the automatic detection of phishing websites, providing an efficient and scalable solution to mitigate such cyber threats. This system captures the important patterns in URLs and the attributes of websites by following the technique of feature engineering, which were used to feed the machine learning models with classifications. The most important features checked were the use of suspicious domains, which leads to misleading URLs, inconsistent or unregular structure of the page, and the usage of obfuscation techniques. Models were evaluated using metrics such as F1 score and area under the receiver operating characteristic curve (AUC-ROC), showing good generalization to new data and high accuracy for detection. The study also compares the computation efficiency and detection performance of various machine learning algorithms, identifying the most efficient model for real-time phishing website detection. The work concludes by highlighting the potential of integrating these machine learning-based detection systems with web browsers and security instruments to protect end-users against real-time phishing attacks through an automated and scalable solution

Keywords: *Phishing Detection, Prediction Algorithms, Support Vector Machines (SVM), Real-Time Detection, Evaluation Metrics (Accuracy, Precision, Recall).*

How to Cite: Sunil Kumar B.; Aditya Kiran; Varun E.; Raghavendra D. Hegde; Dev Vijay Fuletra; Kunal Ittigi. (2025). Machine Learning-Driven Phishing Detection: A Robust Browser Extension Solution. *International Journal of Innovative Science and Research Technology*, 10(3), 988-991. https://doi.org/10.38124/ijisrt/25mar670.

I. INTRODUCTION

The rapid expansion of the Internet and online services has brought about significant changes in communication, business, and entertainment, but it has also introduced new risks. One of the most dangerous threats today is phishing, where attackers deceive users into providing sensitive information like identity details, credit card numbers, and other personal data by pretending to be legitimate entities. Phishing websites mimic genuine ones to steal information. Cybersecurity data indicates that phishing is a major cause of data breaches. Attackers have become highly sophisticated, making their actions hard to detect. They target various platforms, including corporate portals, e- commerce sites, email services, and social media, using deceptive URLs and cloaking techniques that resemble authentic addresses. As these methods continue to evolve, traditional security measures like URL blacklists and heuristics are becoming less effective. This situation creates vulnerabilities, highlighting the urgent need for flexible and scalable solutions that can identify and combat these phishing threats effectively.

II. LITERATURE REVIEW

The proliferation of phishing websites on the internet has led to increased identity theft, financial fraud, and data breaches. Traditional methods like blacklisting and rule-based filters are no longer sufficient to identify these sophisticated phishing sites. Recent research indicates that machine learning has become a highly effective approach for the automatic detection of phishing sites, based on their unique characteristics. Examples of these approaches include feature extraction for phishing detection, supervised machine learning models, deep learning techniques, and hybrid and ensemble methods.

III. DESIGN AND METHODOLOGY

The proposed model works using different phases of execution which are appropriately demonstrated in the figure given below. The figure demonstrates the process right from the start where the user provides a webpage. The multiple phases are listed below.

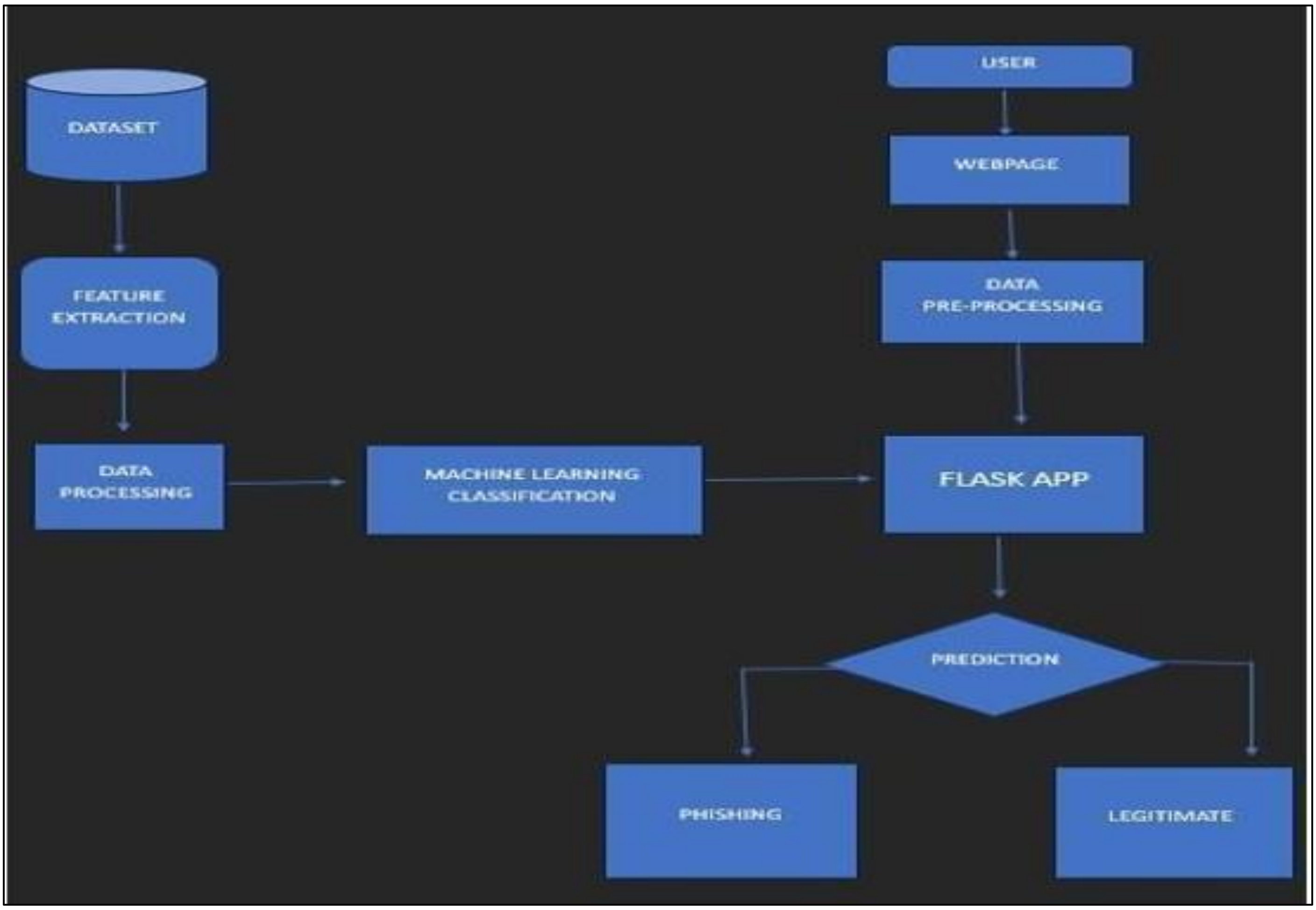


Fig 1: Flow Diagram for Mod

- **Front-end**: The user interface has been crafted with HTML, CSS, and JavaScript to enhance usability. It incorporates various icons and styles to ensure that alerts are visually appealing and easy to understand. The backend logic for detecting phishing links is implemented using Python and Flask. This system utilizes a prediction model specifically trained to distinguish between fraudulent websites and legitimate ones. Further details about these prediction systems will be provided in the following sections.
- **Machine Learning Model:** The respective systems use a Support Vector Machine (SVM) classifier to identify the phishing link. The model is trained on the known dataset of phishing and valid URLs. The system exposes an API that is used by the frontend to submit URL for processing; the API then processes the URLs and returns the result of classification. The alert system then goes ahead to send alerts from the system once a phishing link has been discovered.
- **Data Storage**: The application relies on a database to store the stores' URLs alongside their related categorizations, for future reference and analysis.

This is a model that can be used and deployed as a novel web- based extension in browsers so that it can detect and provide alarms in real time this can be useful as people are surfing the internet around the world.

IV. IMPLEMENTATION

The backend of the project employs a predictive learning model specifically trained to identify phishing websites. This involves extracting features from URLs, such as domain length, presence of special characters, and the inclusion of certain keywords. These features are crucial for training the Support Vector Machine (SVM) classifier to differentiate between phishing and legitimate URLs.

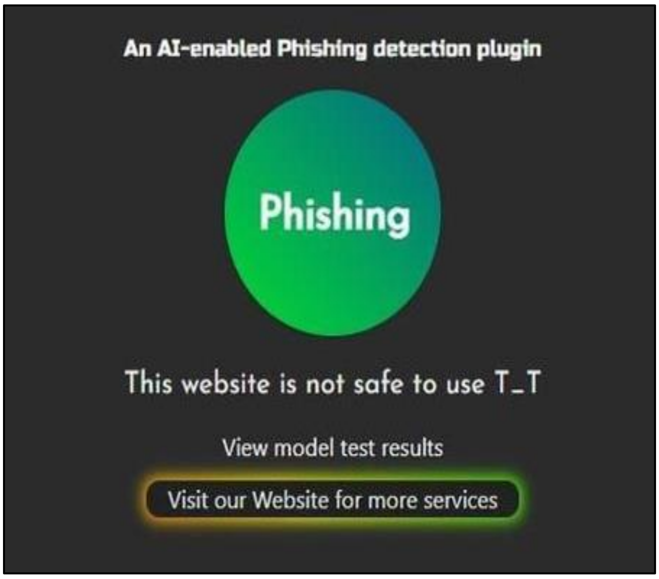
➢ *Key Features used in this Model Include:*

- URL length
- Number of subdomains
- Presence of an IP address in the URL
- Use of the HTTPS protocol
- Presence of special or encoded characters
- Keyword analysis (e.g., terms like "login," "verify," etc.)

When the model identifies a URL as phishing based on these features, the system triggers an alert to the user. This alert system is integrated with various communication channels, such as SMS and email, to ensure timely notifications. Alerts provide detailed information about the threat and recommended actions to protect against phishing attacks. The model is designed to be deployed as a browser extension, offering real-time phishing detection as users browse the web. Deployment involves packaging both the frontend and backend components, along with the machine learning model, into a format compatible with popular web browsers.

V. RESULTS AND ANALYSIS

The system was tested on a database of URLs that were not available at runtime. Performance metrics used include precision, recall, and F1 score. These metrics show that the system can correctly identify phishing URLs while minimizing the negative impact. 95.6% URL accuracy was achieved. This high accuracy demonstrates the model's performance in correctly identifying phishing attempts. Detection now ensures that users are immediately alerted to threats, thus increasing their online provides an additional layer of security without affecting their counter these threats, future work should focus on implementing activities high Accuracy, Real time detection and Browser Extension Deployment are the most important aspects of the project.



An AI-enabled Phishing detection plugin

This website is not safe to use T_T

Fig 2: Example for Web-Based Extension

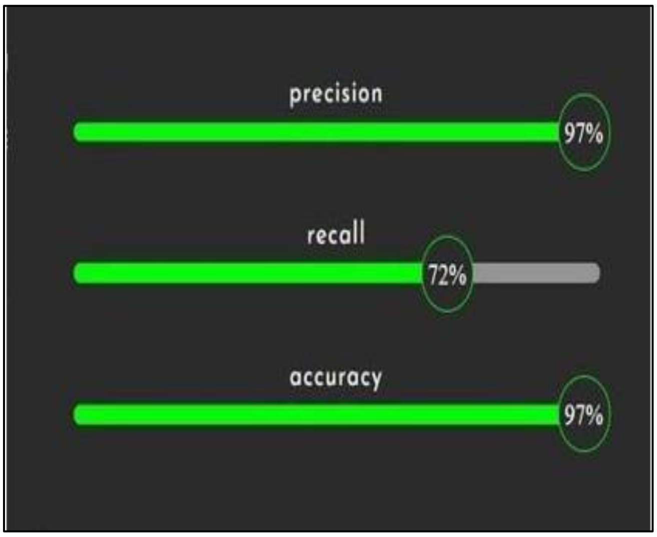


Fig 3: Accuracy of Model

VI. DEPLOYMENT CONSIDERATIONS

Deploying the model in the real world involves several key actions to protect against phishing attacks. Scalability is crucial to handle a high volume of URL requests, and the model is designed for real-time deployment as a browser extension. Implementing robust security measures is essential to safeguard user data and protect the machine learning models from attacks. Regular updates and ongoing training are necessary to enhance accuracy and minimize drawbacks. Enhancing user experience by providing immediate feedback and clear notifications is vital. Integration across various platforms through flexible APIs is important, as is ensuring compliance with cybersecurity laws and ethical standards to prevent misuse. Real-time monitoring and regular adjustments are needed to maintain performance. Educating users about phishing threats and offering strong support can increase awareness and readiness. Collectively, these measures ensure that phishing detection remains effective, efficient, and secure. Continuous improvement and adaptation to new threats are essential for maintaining the system's effectiveness.

VII. CONCLUSION

This model marks a significant leap forward in combating phishing attacks, which pose serious risks to individuals and organizations globally. By utilizing artificial intelligence and machine learning, the model offers a proactive and robust solution for detecting and alerting users to potential phishing threats. Unlike traditional security measures that depend on static rules and signature-based detection, this AI-driven approach can adapt and evolve to counter new and sophisticated phishing tactics. This adaptability is essential in today's dynamic digital landscape, where cybercriminals constantly develop new methods to circumvent traditional defenses.

The model's seamless integration with various digital platforms enhances its effectiveness, ensuring comprehensive protection across multiple communication channels such as emails, social media, and instant messaging applications. This multifaceted protection is crucial for addressing the diverse methods through which phishing attacks can occur. Additionally, the user-centric design makes it easy for non-technical users to benefit from advanced phishing detection capabilities.

By automating the identification and response process to phishing threats, the model not only reduces the risk of financial losses and data breaches but also lessens the burden on IT and cybersecurity teams, allowing them to concentrate on more strategic tasks. In summary, this model represents a forward- thinking approach to cybersecurity, offering a scalable, efficient, and effective means of protecting against the evolving threat of phishing. Its deployment is set to significantly enhance digital security for users across various sectors.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar670

FUTURE WORK

Sophisticated phishing attacks present significant challenges due to their continuously evolving techniques and targeted approaches. These attacks, which include zero-day phishing, highly personalized spear phishing, and the use of encrypted URLs or complex redirects, often evade traditional detection methods. Furthermore, phishing through unconventional channels such as QR codes and social media adds to the complexity of detection. To address these threats, future efforts should focus on implementing advanced machine learning models like deep learning and adversarial training for improved classification accuracy. Expanding the feature set to incorporate behavioral and content analysis, supporting multiple languages, and integrating real-time threat intelligence will enhance detection capabilities. Cross-channel detection and user feedback mechanisms will offer comprehensive protection. Continuous updates and adherence to privacy and ethical standards are crucial to adapting to new phishing tactics, ensuring robust and resilient defenses.

REFERENCES

[1]. Sayeedakhanum Pathan, Ojasvi Maddala, Naga Durga Saile.K and Preety Singh, ” Phishing Websites Detection using Machine Learning”, 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)

[2]. Areti Nagendra Soma Charan, Yu-Hung Chen, and Jiann- Liang Chen. “Phishing Websites Detection using Machine Learning with URL Analysis”, 2022 IEEE World Conference on Applied Intelligence and Computing

[3]. A.Bhavani, R. Sai Lakshmi, P. Harshavardhini, P. Vijay Prakash, N. Vamsi Behara, V. Ajay Kumar, “Detection of Legitimate and Phishing Websites using Machine Learning” Proceedings of the International Conference on Sustainable Computing and Smart Systems (ICSCSS 2023)

[4]. Mahajan Mayuri Vilas, Kakade Prachi Ghansham, Sawant Purva Jaypralash, Pawar Shila, “Detection of Phishing Website Using Machine Learning Approach”, 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)

[5]. Sudhir Anakal, Kiran Maka, Arun Tadkal, Sunil Humanabad, Sridhar Anakal, Laxmikant E, “Phishing Website Detection Using Machine Learning Methods”, 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS)

[6]. Swathi.Y, Swathi.Y, Sravani.P, Pragati Hegde, “Detection of Phishing Websites Using Machine Learning”,2023 International Conference on the Confluence of Advancements in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM).