International Journal of Novel Trends and Innovation
IJNTI.ORG | ISSN : 2984-908X
An International Open Access, Peer-reviewed, Refereed Journal

PhishProbe - Phishing Site Detection Using ML :A Novel Approach Using Generative AI and Streamlit

Punit Gavali

Artificial Intelligence
and Data Science
Fr. Conceicao Rodrigues
College of engineering,
Bandra
Mumbai Maharashtra

Anwaya Belwalkar

Artificial Intelligence
and Data Science
Fr. Conceicao Rodrigues
College of engineering,
Bandra
Mumbai Maharashtra

Abstract— Phishing assaults are becoming more complex, frequently outperforming conventional techniques in terms of detection. In order to lessen these risks, this study offers a novel strategy that integrates generative AI and machine learning into a Streamlit interface. The suggested system provides an adaptable security mechanism that changes in tandem with cybercriminals' strategies by using cutting-edge machine learning techniques to proactively scan and detect phishing websites. We thoroughly evaluate the effectiveness of several machine learning models in correctly detecting phishing websites. In addition, we outline how this solution will be deployed on AWS to improve end-user usability and accessibility.

I. INTRODUCTION

This study offers a novel method to improve phishing site detection by utilizing generative AI and machine learning. By analyzing large datasets, machine learning has the ability to reveal new patterns that human analysts might not see right away. This method maintains a proactive security posture by using generative AI to simulate phishing attacks, which provides insights into the changing tactics of cybercriminals. We highlight the need for creative cybersecurity solutions and list the drawbacks of the detection techniques used today. This study promotes the use of cutting-edge machine learning methods to comprehend and identify phishing websites, offering a flexible security system that can react to ever-changing online threats. Our method not only overcomes the shortcomings of current detection systems but also advances artificial intelligence applications in cybersecurity more broadly.

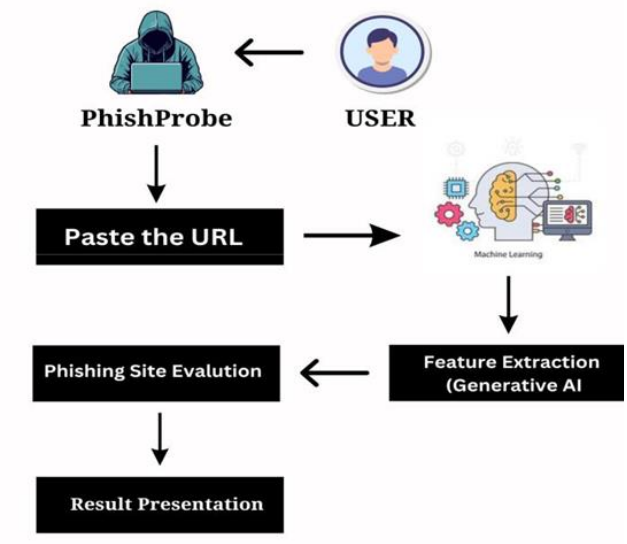

Fig. 1 System Architecture

A. Significance of StreamLit

Streamlit is essential to our project because it makes it easier to quickly build and implement an intuitive user interface for the machine learning-based phishing detection tool. Its ease of use allows for quick iterations, which is crucial for dealing with the ever-changing cybersecurity environment. Streamlit's smooth integration into the Python ecosystem gives it direct access to data science libraries, which improves the tool's capacity to accurately assess and anticipate phishing threats.

B. Purpose and Scope of the Research

The goal of this project is to create a sophisticated machine learning tool for phishing website identification in order to combat the growing threat of cyberattacks. The research aims to provide consumers with a proactive defensive mechanism against phishing assaults by incorporating generative AI into an intuitive Streamlit interface. The study covers the creation, use, and assessment of the detection system, including performance evaluation, algorithm selection, dataset collection, and user interface design. Delivering a complete solution that increases detection accuracy and guarantees usefulness in real-world applications is the goal in order to foster a more secure online environment.

C. Research Questions

To meet the research objectives, the following key questions are addressed:

1. How effective is the proposed machine learning approach in comparison to traditional phishing detection methods?
2. In what ways does generative AI enhance phishing site detection capabilities?
3. What security measures are essential to safeguard transaction integrity within the platform?
4. How does user perception of this solution compare to that of existing alternatives?

II. LITERATURE REVIEW

A. Evolution of Phishing Detection Techniques

Techniques for detecting phishing attacks have changed dramatically over time, moving from manual, rule-based systems to sophisticated machine learning-driven ones. Early detection techniques, which at first relied on human awareness to spot dubious emails or websites, had limitations in terms of scalability and efficacy against phishing tactics that were becoming more complex. The quick iterations necessary to handle the rapidly evolving nature of cybersecurity threats are made possible by the integration of Streamlit with Python modules, which enables the quick building of user-friendly interfaces.

B. Phishing Detection Using Machine Learning

The advent of machine learning was a significant advancement in phishing detection since these algorithms can recognize intricate patterns in large datasets. Machine learning algorithms boost cybersecurity defences by analyzing vast amounts of data and accurately identifying tiny signs of phishing.

C. Gaps in Current Research

There is a discernible lack of study on the technical and usability aspects of implementing Streamlit-based phishing

detection systems, despite the large number of papers investigating phishing detection and machine learning. The effectiveness of machine learning in phishing detection has been shown in earlier research, but few studies have looked at the real-world effects of incorporating these technologies into user-friendly platforms like Streamlit. By offering a thorough analysis that successfully improves cybersecurity measures by fusing technical rigor with user-centric design principles, this study aims to close this gap.

III. THEORETICAL FRAMEWORK

A. Phishing Detection Using Machine Learning

Few studies have carried out a thorough analysis that takes into account both technical implementation and usability, especially within Streamlit-based systems, even if previous research has examined the relationship between phishing detection and machine learning. By offering a comprehensive analysis that strengthens cybersecurity measures by fusing technical rigor with user-centric design principles, this research fills this gap.

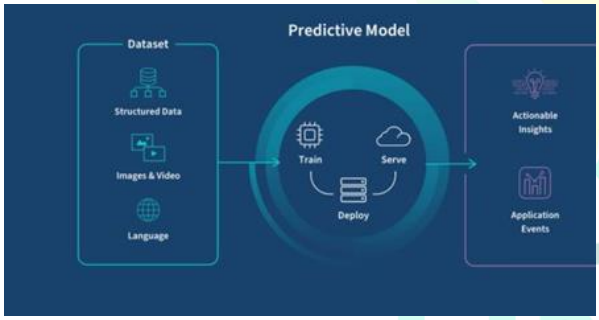

Fig. III (A) Predictive Model

B. Streamlit

A Machine Learning User-Friendly Interface—A Python package called Streamlit makes it possible for programmers to quickly and easily create interactive web apps that are suited for data science and machine learning projects. Because of its user-friendly interface, non-technical individuals can now engage with machine learning models and view outcomes in real time, making sophisticated algorithms more accessible. Developers can easily combine data visualizations, interactive user input elements, and machine learning models into a single application with Streamlit. In a variety of domains, including cybersecurity, this user-centered design greatly improves the usability and accessibility of machine learning systems. Therefore, Streamlit is a useful tool for bridging the gap between machine learning applications' technical complexity and user engagement.

Fig III (B) Streamlit Workflow

C. Using AWS to Implement Machine Learning Models

A wide range of cloud computing solutions are available from Amazon Web Services (AWS) to help with machine learning model deployment, scaling, and management. Developers can implement machine learning models in a scalable, economical way while guaranteeing peak performance and dependability by utilizing AWS's strong infrastructure. Comprehensive model deployment needs are supported by AWS services, such as Amazon SageMaker for training and deploying models, Amazon EC2 for hosting web applications, and Amazon S3 for storing data and models. Furthermore, AWS uses robust security features like access controls and encryption to shield private information and apps from online attacks. Thus, by using AWS for model deployment, businesses may successfully improve their cybersecurity defenses against phishing assaults by utilizing cloud computing capabilities.

D. Streamlit and AWS Integration for Phishing Detection

By producing synthetic data that closely mimics real phishing websites, generative AI platforms—like Google's GenAI (Gemini)—represent a significant leap in phishing detection skills and improve cybersecurity. By allowing machine learning models to catch subtle phishing-related traits and patterns, this synthetic data helps to improve the models. These algorithms become more accurate at differentiating between authentic and counterfeit websites by better identifying subtle phishing cues. By integrating these platforms with AWS and Streamlit infrastructure, businesses may take advantage of generative AI's promise to strengthen cybersecurity protections.

IV. METHODOLOGY

A. System Requirements

1. Streamlit: Streamlit offers a user-friendly interface for engaging with the phishing detection system, making it simple for users to submit URLs for examination and get prompt confirmation of each website's validity.
2. Amazon Web Services (AWS): The machine learning-based phishing detection system is hosted by Amazon Web Services (AWS), which guarantees scalability, dependability, and wide accessibility. The system can support a large user base and efficiently handle fluctuating traffic volumes thanks to its AWS deployment.
3. Python Libraries: To create and implement the system, a variety of Python libraries are used, such as:
    a. Scikit-learn: Offers the fundamental tools for creating a strong phishing detection model and is used for putting machine learning algorithms into practice and evaluating models.
    b. NLTK (Natural Language Toolkit): In order to increase user confidence in the system's predictions, NLTK (Natural Language Toolkit) is used to improve the visual feedback. Phishing websites are shown by red markers, whereas trustworthy websites are indicated by green ones.
4. Google’s Gen AI: Google's Generative AI technology is integrated for sophisticated feature With the help of sophisticated feature extraction and sophisticated natural language processing and pattern identification, Google's Generative AI technology allows for the analysis of website content, structure, and activity. By using Gen AI, the system finds subtle signs of phishing activity that traditional detection methods can miss.

Fig .VI (Requirements of system)

B. Process

- Analysis Input URL: To start the analysis, users input a URL into the Streamlit interface.
- Feature Extraction: To extract pertinent features from the website content, the system uses generative artificial intelligence (AI) approaches, such Google's Gen AI. The model's capacity to correctly identify phishing sites is improved by this extraction procedure, which records a thorough comprehension of the webpage's structural components, content semantics, and behavioral patterns.
- Phishing Site Evaluation—A machine learning model hosted on AWS processes the features that were extracted. The model assesses the feature set and makes predictions about the website's legitimacy or possible phishing danger using Scikit-learn. High performance and dependability are ensured by Scikit-learn's support for

a variety of machine learning algorithms and model evaluation methodologies.

V. ALGORITHMS

1. Logistic Regression: A statistical method used to analyze datasets with one or more independent variables that influence an outcome variable. The model achieved an accuracy of 70.3%.
2. Support Vector Machine (SVM) Classifier: A supervised learning algorithm that identifies the optimal hyperplane to separate data points into distinct classes. The classifier reached an accuracy of 70.9%.
3. Decision Tree: A tree-like structure in which each internal node represents a test on an attribute, each branch denotes the result of the test, and each leaf node signifies a class label. The model achieved an accuracy of 77.2%.
4. Random Forest: An ensemble learning technique that generates multiple decision trees during training and outputs the class mode for classification or the average prediction for regression. This model attained an accuracy of 81.3%.
5. Gaussian Naive Bayes: A probabilistic classifier based on Bayes' theorem, which assumes strong independence between features. The model achieved an accuracy of 66.4%.
6. XGBoost: An optimized implementation of gradient-boosted decision trees designed for performance and computational efficiency. Widely used in competitive machine learning, it achieved an accuracy of 80.9%.
7. AdaBoost: Adaptive Boosting combines multiple weak classifiers to form a robust classifier. The model attained an accuracy of 75.95%.
8. Gradient Boosting: A technique for both regression and classification that builds models sequentially by minimizing a loss function through gradient descent. This model reached an accuracy of 77.9%.

Ensemble Learning Techniques

1. Bagging Classifier: An ensemble method that creates multiple instances of a base model using bootstrapped samples of the training data, combining predictions through averaging (for regression) or voting (for classification).
2. Stacking Classifier: An ensemble technique that combines several classification models using a meta-classifier. Base models are trained on the initial dataset, and their predictions serve as features for a higher-level model.

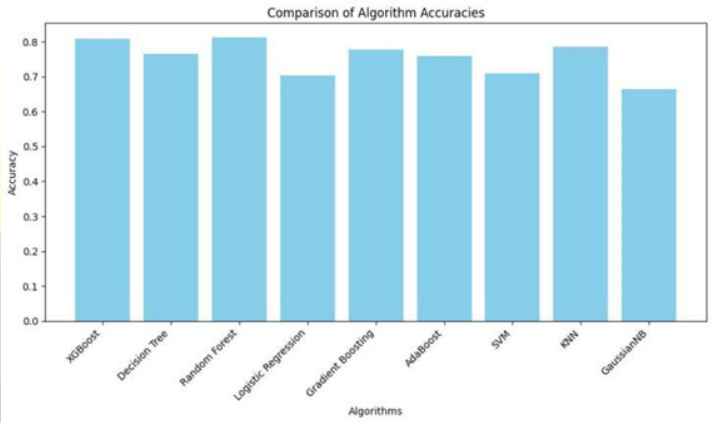

Fig. V Comparison of Algorithms

VI. RESULTS

Fig. V(A) Spam

Fig. V (B) Not Spam

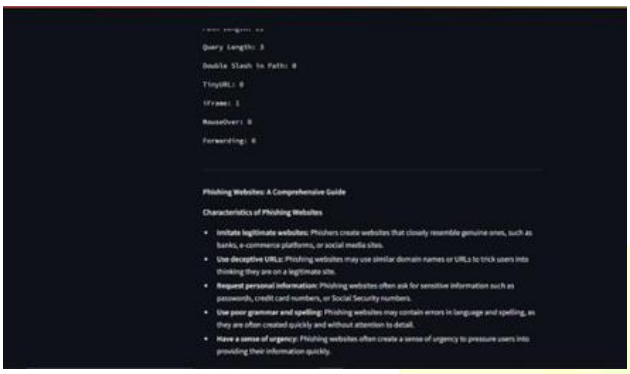
Fig. V (C) Gen AI

Fig. V(D) Feature Extracted

VII. SOCIAL RELEVANCE AND MARKET REVIEW

A. Social Relevance.

1. Enhanced Cybersecurity: In today's digital world, there is an urgent need for improved cybersecurity, which is addressed by the suggested machine learning-based phishing detection system, which was created on Streamlit and hosted on AWS. It greatly aids in the protection of sensitive data and protects people and businesses from financial loss and data breaches by providing users with proactive defense mechanisms.
2. Usability and Accessibility: This system democratizes access to advanced cybersecurity technologies by utilizing Streamlit's user-friendly and intuitive interface, which makes them accessible to a wider range of users. Because of this inclusion, people with different technical backgrounds can successfully improve their digital security.
3. Proactive Defense Against Changing Threats: Our strategy employs machine learning and generative artificial intelligence (AI) to foresee and thwart emerging cybercriminal tactics as phishing techniques continue to progress.
4. Encouraging Decision-Making: The system assists users in making well-informed judgments in the internet sphere by giving them immediate feedback on the legitimacy of websites. A culture of digital resilience and ethical online conduct is promoted by enabling people and organizations to critically assess online sources and steer clear of phishing risks.

B. Market Review

Growing Phishing Attack Threats: People and businesses are at serious risk due to the global rise in phishing assaults. The market for advanced cybersecurity solutions that can successfully detect and stop phishing is expanding as fraudsters employ increasingly complex strategies to steal sensitive data.

Technological Developments in Cybersecurity: Machine learning and artificial intelligence (AI) have made major strides in the cybersecurity sector, particularly in the areas of threat identification and response. Building on these developments, our system offers a proactive, efficient phishing detection solution. The trend toward cloud-based cybersecurity solutions that provide scalability, flexibility, and accessibility is a result of the increasing popularity of cloud computing. Our system's deployment on AWS takes advantage of these advantages, guaranteeing dependable performance and easy access from a variety of devices and places.

Growing Demands for Compliance and Awareness: Regulations like GDPR, HIPAA,

and PCI DSS place a strong emphasis on security measures as cybersecurity awareness grows. By complying with these compliance criteria, our phishing detection technology gives businesses a proactive way to safeguard confidential data and adhere to legal regulations.

Need for User-Friendly Solutions: As cybersecurity threats become more sophisticated, there is a growing need for solutions that are easy to use and enable individuals and organizations to defend themselves. The phishing detection system is easier to use and more widely adopted by a variety of demographics because to Streamlit's user-friendly design.

Global Reach and Market Expansion: In the linked world of today, cybersecurity risks cut across national boundaries and impact people and enterprises everywhere. Our solution, which is hosted on AWS, guarantees worldwide accessibility and scalability, satisfying the cybersecurity requirements of customers in many industries and geographical areas. Its broad reach increases its worth for businesses looking for strong phishing prevention in the worldwide digital environment.

VIII. CONCLUSION

To sum up, our machine learning-driven phishing detection solution, which is hosted on AWS for scalability and Streamlit for an interactive interface, represents a major advancement in the cybersecurity space. By providing an easy-to-use platform that aids in distinguishing between trustworthy and fraudulent websites, this system empowers the user. After extensive testing, we found that the Stacking Classifier model with certain features produced the best classification accuracy of 81.55% for successfully identifying phishing sites.

The accuracy of our model across a range of algorithms demonstrates its resilience:

- XGBoost: 80.95%
- Decision Tree: 76.60%
- Random Forest: 81.25%
- Logistic Regression: 70.30%
- Gradient Boosting: 77.85%
- AdaBoost: 75.95%
- SVM: 70.90%
- KNN: 78.65%
- GaussianNB: 66.45%

Furthermore, by combining Stacking Classifiers and Extra Trees, we were able to attain an accuracy of 82%. These findings demonstrate how well the algorithm classifies URLs as either legitimate or fraudulent, offering a dependable defense against phishing attacks.

Key Metrics Achieved

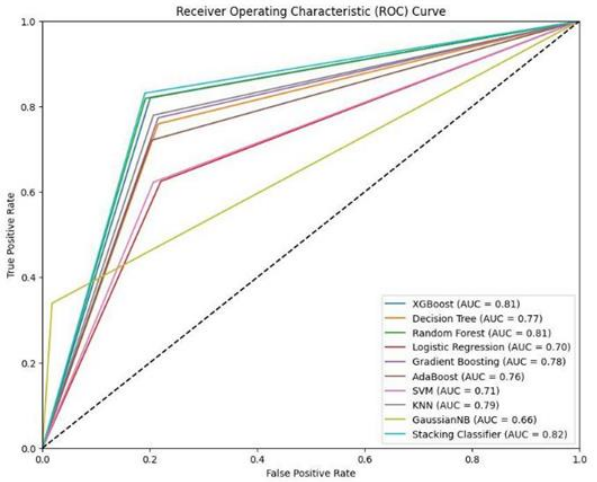

Fig. VIII ROC Curve

1. Accuracy (0.8135): About 81.35% of the cases were properly classified by the model.
2. Precision (0.8066): There was a high degree of accuracy in identifying phishing sites, with approximately 80.66% of phishing predictions being correct.
3. Recall (0.8188): The model's ability to identify phishing threats is demonstrated by the fact that 81.88% of real phishing sites were accurately identified.

Therefore, this research serves as an example of how generative AI and machine learning may be used to improve cybersecurity and provide users the skills they need to successfully traverse the constantly shifting digital terrain.

REFERENCES

[1] Lakshmanarao, A., Rao, P.S.P., Krishna, M.M.B. (2021) 'Phishing website detection using novel machine learning fusion approach', in 2021 International (ICAIS)

[2] H. Chapla, R. Kotak and M. Joiser, "A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifer", 2019 International Conference on Communication and Electronics Systems (ICCES), pp. 383-388, 2019, July

[3] Vaishnavi, D., Suwetha, S., Jinila, Y.B., Subhashini, R., Shyry, S.P. (2021) 'A Comparative Analysis of Machine Learning Algorithms on Malicious URL Prediction', in 2021 5th (ICICCS), 1398–1402

[4] Dinesh P.M, Dr. Mukesh M; "Identifcation of Phishing Attacks Using Machine Learning Algorithm"; Volume 9, Issue 4 (2022)

[5] Abu-Nimeh, S., Nappa, D., Wang, X., Nair, S. (2007), A comparison of machine learning techniques for phishing detection. Proceedings of the Anti-phishing Working Groups 2nd Annual ECrime Researchers Summit on - ECrime '07.

[6] Sharma, Ushamary and Ghisingh, Seema and Ramdinmawii, Esther, "A Study on the Cyber - Crime and Cyber Criminals: A Global Problem," International Journal of Web Technology, vol 03, pp. 172-179, June 2014.

[7] Vayansky, I. and Kumar, S., "Phishing – challenges and solutions.", Computer Fraud & Security, vol 2018, no. 1, pp. 15-20, January 2018.

[8] Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. "Machine Learning-Based Phishing Detection from URLs," Expert Systems with Applications, vol. 117, January 2019