AMRITANETRA
(Amrita Network Threat Recognition and Analysis)

Darshan Suresh, Vidhyadhara M
UG Student Department of Computer Science,
School of Computing, Amrita Vishwa Vidyapeetham, Mysuru.

Supervisor:
Dr. Adwitiya Mukhopadhyay
Deputy Controller of Exams,
Amrita Vishwa Vidyapeetham, Mysuru.

Major Project -20CSA399

ABSTRACT

Phishing threats still pose danger to users by impersonating genuine sites to harvest secure information. AmritaNetra (Amrita Network Threat Recognition and Analysis) is an AI-based system that identifies phishing attacks through supervised machine learning and URL feature extraction. It distinguishes itself through the incorporation of a chatbot and storytelling engine powered by AI to inform users of probable attacks in real time. With up to 97.5% precision achieved using CatBoost, the system provides powerful predictive capability in conjunction with innovative user engagement. AmritaNetra is an authentic, user-informed, safe solution to advanced phishing mitigation and cyber-awareness.

INTRODUCTION

OBJECTIVES

- Design a phishing detection system to detect suspicious URLs using machine learning method.
- Extract and utilize various web feature and URL-based features in an effort to predict sites as phishing or legit.
- Compare and analyze various supervised learning models for selecting the best model to operate effectively with maximum precision.
- Optimize for real-time prediction in minimum response time for real-world field deployment.
- Use a threat-communicating chatbot that communicates plainly and educates for a safer internet.
- Use a story-telling AI module to tell users phishing stories so they can more easily remember and learn from threats.
- Encourage user education and cybersecurity awareness through interactive, interactive components in the app.

SCOPE

- Detect phishing websites accurately using machine learning techniques.
- Assist users with real-time threat alerts and explanations via chatbot.
- Improve cybersecurity awareness through AI-generated storytelling.
- Offer an interactive and educational experience beyond simple detection.
- Ensure the system is scalable for integration with browsers or web applications.

PROPOSED SYSTEM

Preprocessing of Data for Phishing Detection Models:
We employ the Kaggle phishing dataset of 11,054 web instances, labeled as phishing (1) or legitimate (-1). The dataset has 30+ features such as URL length, presence of HTTPS, domain age, and anchor tags. Data is cleaned and normalized, and the 'Index' column is removed. There are no missing values.

Model Architecture:
We test several models: Logistic Regression, K-Nearest Neighbors, SVM, Decision Tree, Random Forest, Gradient Boosting, and CatBoost. Gradient Boosting is selected because of its improved performance (accuracy: 97.4%). Models are trained on an 80-20 train-test split and evaluated using F1-score, accuracy, recall, and precision.

AI Storytelling and Chatbot Integration
The system has an AI-driven narrative module that provides details of the identified phishing attacks in the form of dynamic stories. A chatbot delivers real-time phishing detection, awareness training, and phishing attempt simulation for training. The double integration guarantees improved usability and user interaction, which differentiates AmritaNetra from existing systems.

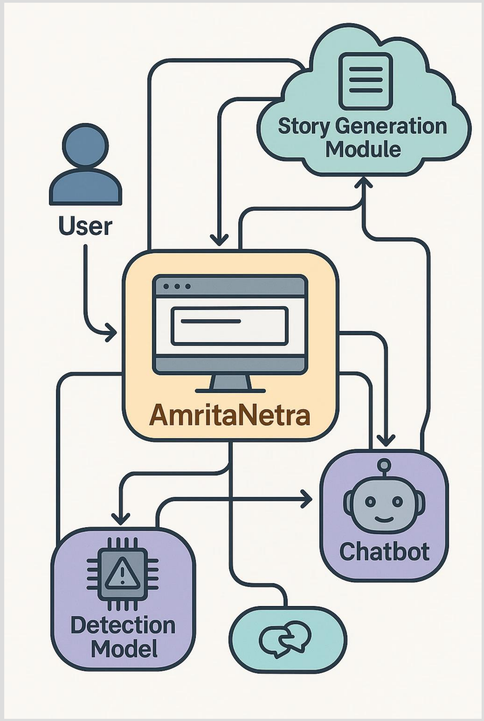

Figure 1. System Overview Diagram

SAMPLE OUTPUT INTERFACE

The AmritaNetra system was tested using real-world URLs. For each input, the model predicted whether the URL was phishing or legitimate. A successful phishing detection triggered a chatbot warning and a brief AI-generated story to educate the user.

Quantitative Results

Example output:

- Input URL: http://secure-login.example.com
- Prediction: Phishing
- Confidence Score: 98.7%
- Model Used: CatBoost
- Response Time: 0.28 seconds

Qualitative Results

The chatbot explained the risks clearly, and the storytelling module narrated a phishing incident similar to the input case, improving user understanding and awareness.

Test Case	Input URL	Prediction	Chatbot Response Summary	Story Generated Summary
TC-01	http://secure-login.example.com	Phishing	Warns about suspicious URL structure and missing HTTPS.	Story about a user tricked by a similar fake login page.
TC-02	https://bankofindia-secure.info	Phishing	Alerts user about lookalike domain and recent phishing patterns.	Story of a financial scam involving a forged banking domain.
TC-03	https://accounts.google.com	Legitimate	Confirms the site is verified and safe to proceed.	No story generated.
TC-04	http://mail-auth.xyz	Phishing	Highlights risk due to shortened domain and unknown source.	Story of identity theft caused by email credential phishing.

Table 1. Qualitative Output of AmritaNetra Interface

Figure 2. Phishing website result

Figure 3. Legitimate website result

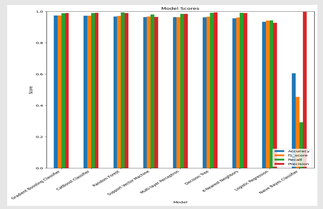

Chart 1. ML Model Metrics Comparison

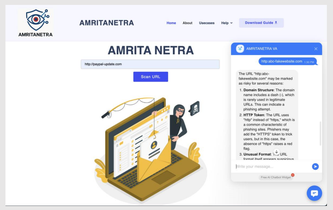

Figure 4. Chatbot Response for Phishing website

CONCLUSION/FUTURE WORK

AmritaNetra displays a strong combination of machine learning and AI-based interaction for phishing site detection. Using a good dataset and experimenting with various supervised models, the system has a very high accuracy percentage, where the best model proves to be Gradient Boosting. The convergence of AI story-telling in an interactive chat interface provides AmritaNetra its distinctness, making it a world-class learning platform which is no longer a passive detection tool. Other than being defended against phishing attempts, users are also trained with live scenarios and chatbot guidance, opening up the way towards digital literacy as well as experiential training.

Future developments would involve expanding the phishing detection functionality of AmritaNetra to social media, mobile applications, and more among other platforms. Embedding Natural Language Processing (NLP) to automatically scan phishing messages and emails for greater security will also be considered. Adaptive learning through a feedback loop of users' reports will also be added so as to continue learning from new phishing trends and threats continuously.

CONFERENCE AND PUBLICATION

REFERENCES

1. **A. Mukhopadhyay and A. Prajwal, "EDITH – A Robust Framework for Prevention of Cyber Attacks in the Covid Era,"** 2021.https://ieeexplore.ieee.org/abstract/document/9456186

2. **A. Mukhopadhyay, V. S. Skanda, and C. J. Vignesh, "An Analytical Study on the Versatility of A Linux Based Firewall From A Security Perspective," 2015.** http://www.ripublication.com

3. **A. Mukhopadhyay et al., "QoS-Aware IoT Edge Network for Mobile Telemedicine Enabling In-Transit Monitoring of Emergency Patients,"** 2024. https://doi.org/10.3390/fi16020052

4. **P. Anusri et al., "Shielding Cyberspace: A Machine Learning Approach for Malicious URL Detection," 2024.** https://ieeexplore.ieee.org/abstract/document/10724442

5. **M. Diviya et al., "Enhancing Cyber Security Through Phish-Net – An Artificial Neural Network for Phishing Detection," 2024.** https://ieeexplore.ieee.org/abstract/document/10699017

6. **A. Sa et al., "An Ensemble Classification Model for Phishing Mail Detection," 2024.** https://www.sciencedirect.com/science/article/pii/S187705092400646X