PHISHING-AWARE: E-COMMERCE WEBSITE WITH NEW FEATURES AND PROTECTION FROM PHISHING

Surendrababu.E[1],Vishnu.K[2],Pavankumar.R[3],Priya.V[4*]
[123]UG Scholar-Dept.CSE,GRT Institute Of Engineering &Technology, Tiruttani, India.
[4]Assistant Professor-Dept.CSE,GRT Institute of Engineering & Technology, Tiruttani, India.
surendrababu.sunil101@gmail.com, k87196287@gmail.com, pavan1610850@gmail.com
***Corresponding Author: priya.v@grt.edu.in**

Abstract

Phishing websites are very dangerous as they exploit the vulnerabilities of people to get access to people's sensitive information and data. These type of websites later pretend to be legitimate sources to deceive users into revealing their personal data. Attackers usually target on the common details like email IDs and credit card numbers being common targets. Detecting phishing kind of attacks is critical because they are becoming more and more hostile. Phishers often choose websites that appear visually and semantically identical to genuine ones. Here the protective measure aims to safeguard users security, prevent access to fake users, hacked, or undesirable URLs, and to give the trust to the users of our website towards their data privacy and protection from the phishing Advertisement.

Keywords: *Review analysis, Product comparison, Phishing detection, Blocking page redirection.*

1. Introduction

Introducing a Phishing-Aware E-commerce Website. Explore the enhanced security and innovative features designed to protect users from phishing threats. Safeguarding your online shopping experience, this platform goes beyond traditional measures, ensuring a secure environment for transactions and user data. Discover the cutting-edge solutions implemented to combat phishing attempts and elevate your online safety.

2. Related Work

This paper discusses the significance of IPv6 and its NDP (Neighbor Discovery Protocol) component in shaping the future of internet connectivity and IT expansion. However, it also highlights the vulnerability of NDP to various cyber attacks due to its trust-based model. To address these security concerns, the paper proposes NDP security (NDPsec) mechanism based on the Ed25519 digital signature. Overall, the paper suggests that NDPsec offers significant advantages in terms of security, processing efficiency, and resilience against cyber attacks compared to existing NDP security mechanisms. This highlights its potential to address the security challenges associated with IPv6 and NDP, thus facilitating the adoption of IPv6 as the cornerstone for future internet connectivity and IT expansion.[1]

This paper addresses the persistent issue of phishing attacks in the digital world and proposes a novel approach to counter them using multilayered stacked ensemble learning. Proposed Approach: The paper introduces a multilayered stacked ensemble learning technique, comprising estimators at different layers. Predictions from the current layer's estimators serve as input for the next layer, creating a hierarchical and interconnected model.[2]

This paper addresses the ongoing threat of phishing attacks, wherein attackers employ social engineering techniques to lure users into divulging sensitive information through deceptive websites. To address these challenges, the paper proposes a deep learning-based framework implemented as a browser plug-in. This framework aims to provide real-time detection of phishing risks when users visit web pages, issuing warning messages as necessary. The real-time prediction service integrates multiple strategies, including whitelist filtering, blacklist interception, and machine learning (ML) prediction, to enhance accuracy, reduce false alarms, and minimize computation time.[3]

This paper addresses the persistent challenges in phishing detection despite decades of development, particularly focusing on the potential of deep learning techniques to enhance detection accuracy.Taxonomy Proposal: The study presents a taxonomy of deep learning algorithms for phishing detection by systematically reviewing 81 selected papers. The taxonomy aims to categorize existing literature into various classifications, providing a structured framework for understanding and analyzing the landscape of deep learning techniques in phishing detection.[4]

This paper addresses the persistent threat of phishing attacks and proposes a boosting-based multi-layer stacked ensemble learning model for effective detection. The paper highlights phishing as a prevalent online scam where attackers impersonate trustworthy entities to obtain personal information such as passwords and credit card details. Despite efforts to combat these attacks, they continue to pose a significant threat to users.[5]

3. Objective

The Main motive of this project is to provide an e-commerce service to the user with an fruitful propitious to enhance the user experience while using our e-commerce website. And also safeguarding the user from threads and unwanted type of advertisements like phishing while using our website.

4. Proposed System

Nowadays all are doing purchases through the online shopping only. In current e-commerce website we have limited features and protection of user data's. In our project we developed and implemented new features like product comparison chart views, Giving positive & Negative grade to the user review by Analyzing the review statements given by reviewer. And also protecting the user from the unwanted. Threads & phishing Ads while shopping throw our website.

5. Architecture Diagram

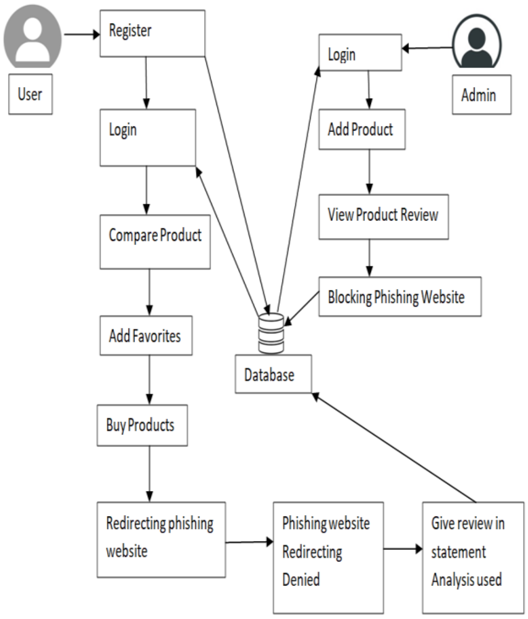

Register
User
Login
Compare Product
Add Favorites
Buy Products
Redirecting phishing website
Phishing website Redirecting Denied
Give review in statement Analysis used
Database
Login
Admin
Add Product
View Product Review
Blocking Phishing Website

Fig: 5.1 Architecture Diagram

6. Implementation

6.1 Social Networks Module

In this module the user login to the application and use search engine to search any content of data. This application get the required data with respective to the keywords entered in the search engine. And also this module include all the basic feature like , add favorite , add to cart, and More.

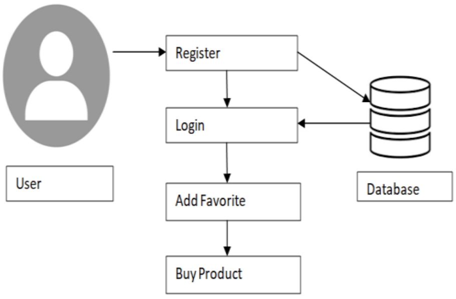


Fig: 6.1 User Activity

6.2 Product Comparison Module

This module includes the comparison feature, this is one of the new feature added in our proposed system.By this comparison feature the user can able to compare the products according to their needs.This feature helpful in faster decision making and to selecting an good product from the available products in the website.

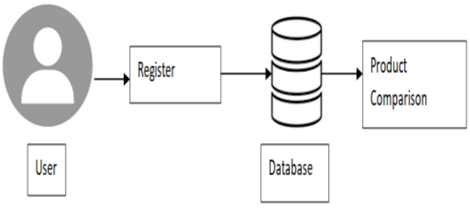


Fig: 6.2 Comparison Process

6.3 Review Analysis Module

This module includes the second new feature of our proposed system.This review analysis feature give rating for the product by analyze the user review word by word by compare it with the good and bad values we given as document as pre- builderedly. This will be helpful in getting the accurate rating percentage for the particular product .

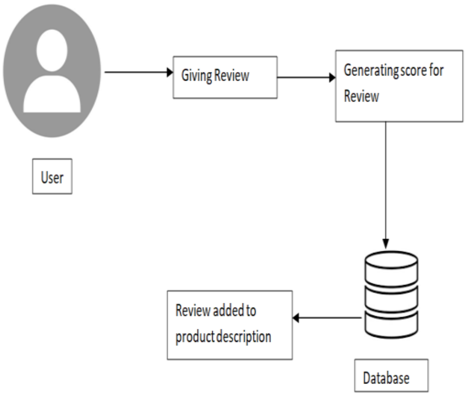

Giving Review
Generating score for Review
User
Review added to product description
Database

Fig: 6.3 Review Score Generating Process

6.4 Admin Module

This module includes all the activities done by the admin team of the web page. The activities are admin login, add product, view product review and more. Majorly detecting and blocking the phishing ads from the website.By this, the users can feel safe to use our E-commerce website.

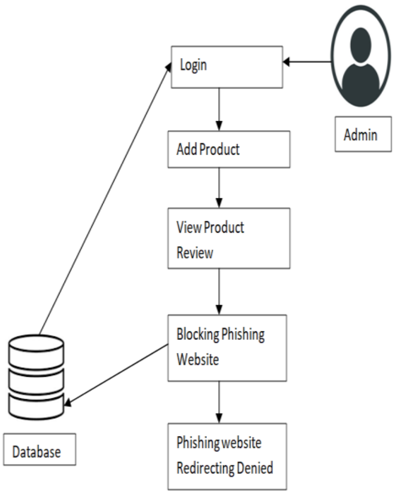
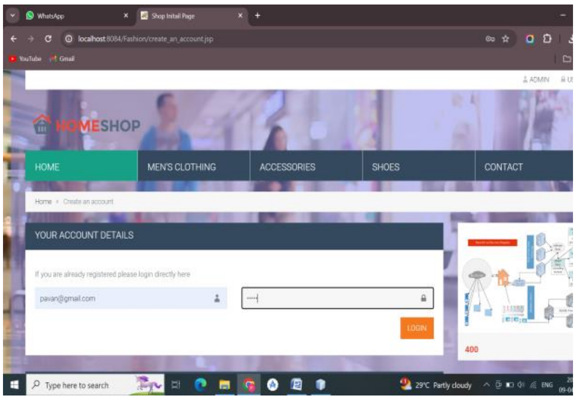

Login
Admin
Add Product
View Product Review
Blocking Phishing Website
Phishing website Redirecting Denied
Database

Fig: 6.4 Admin Controls And Activity

7. Experimental Result

In this result section we discusses about the implementation of new features to the e-commerce website like a product comparison and generating score for user review based on the good and bad values and also identifying and blocking the phishing advertisements figure 7.1 shows the user login and figure 7.2 shows the admin login and figure 7.3 shows product comparison and figure 7.4 shows the review score analysis and finally figure 7.5 showing the phishing advertisement page and blocking page redirection .

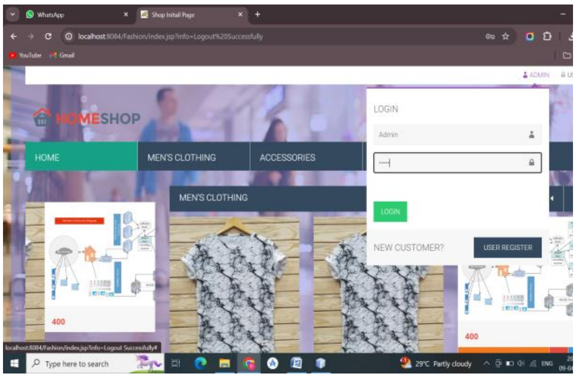


YOUR ACCOUNT DETAILS

If you are already registered please login directly here

pavan@gmail.com

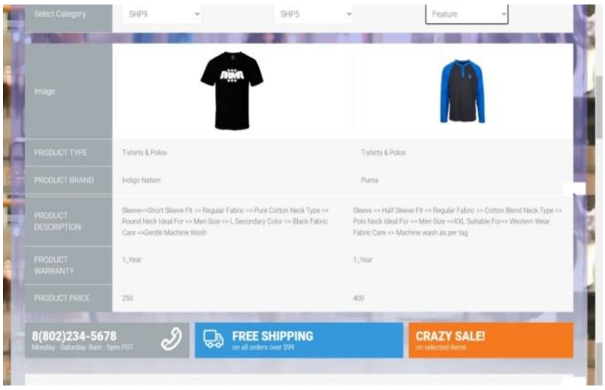
Fig: 7.1 User Registration & Login Page



LOGIN

Admin

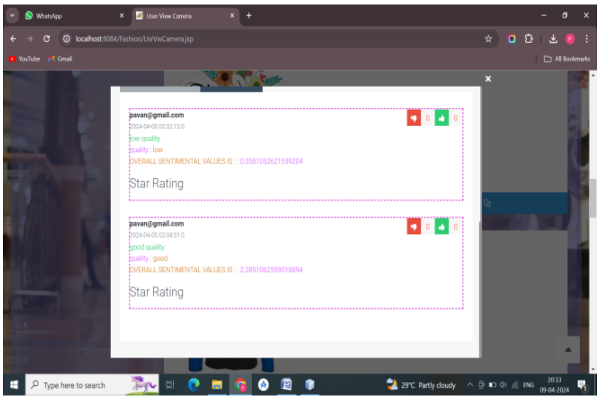
Fig: 7.2 Admin Login Page



Select Category	SHP9	SHP5
Image		
PRODUCT TYPE	T-shirts & Polos	T-shirts & Polos
PRODUCT BRAND	Indigo Nation	Puma
PRODUCT DESCRIPTION	Sleeve=>Short Sleeve Fit => Regular Fabric => Pure Cotton Neck Type => Round Neck Ideal For => Men Size => L Secondary Color => Black Fabric Care =>Gentle Machine Wash	Sleeve => Half Sleeve Fit => Regular Fabric => Cotton Blend Neck Type => Polo Neck Ideal For => Men Size =>XXL Suitable For=> Western Wear Fabric Care => Machine wash as per tag
PRODUCT WARRANTY	1_Year	1_Year
PRODUCT PRICE	250	400

Feature

Fig: 7.3 Product Comparison Page



pavan@gmail.com
2024-04-05 02:02:15.0
low quality
quality : low
OVERALL SENTIMENTAL VALUES IS : : 0.5581052621539204
Star Rating
0 0

pavan@gmail.com
2024-04-05 02:04:51.0
good quality
quality : good
OVERALL SENTIMENTAL VALUES IS : : 2.3891062559018894
Star Rating
0 0

Fig: 7.4 Review Score Analysis Page

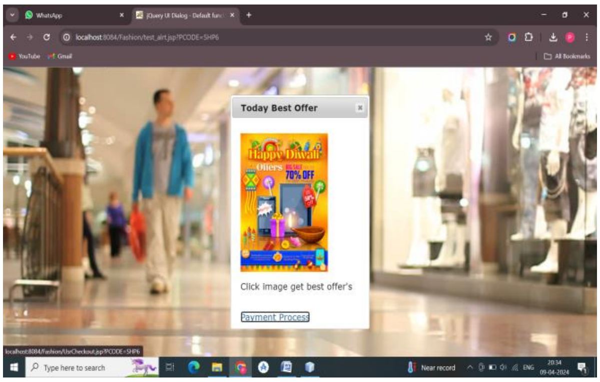
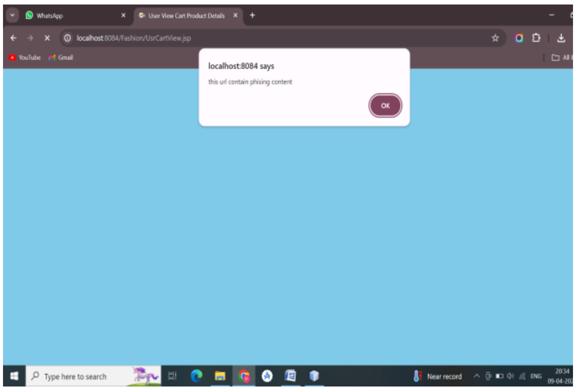

WhatsApp
jQuery UI Dialog - Default func
localhost:8084/Fashion/test_alrt.jsp?PCODE=SHP6
YouTube
Gmail
All Bookmarks
Today Best Offer
Happy Diwali
Offers
70% OFF
Click image get best offer's
Payment Process
localhost:8084/Fashion/UsrCheckout.jsp?PCODE=SHP6
Type here to search
Near record
ENG
20:34
09-04-2024

Fig:7.5 Displaying Advertisement page


WhatsApp
User View Cart Product Details
localhost:8084/Fashion/UsrCartView.jsp
YouTube
Gmail
Type here to search
Near record
ENG

localhost:8084 says

this url contain phising content

OK

Fig:7.6 Blocking From Phishing Page Redirection

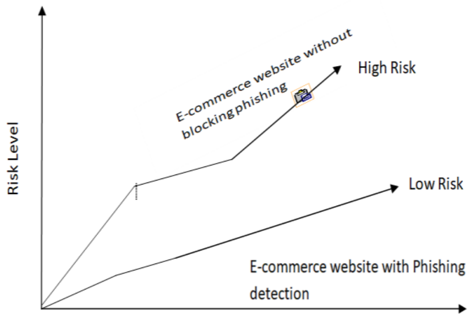


Fig:7.7 Risk Reduction Chart

8. Conclusion & Future Work

By this project we have been initiated new Features in the existing E-commerce in the platform, it would be very helpful for the user to experiences the new features in the shopping Website. And another major features in this project was have implemented security protection for the user personal data from the phishing advertisement in the E-commerce Shopping Website. In Future the Phishing detection will be fully automated in our platform by using some AI and Machine Learning.

9. Reference

1. Ayman Al-Ani , Ahmed K. Al-Ani ,Shams A. Laghari , Selvakumar Manickam Khin Wee Lai , And Khairunnisa Hasikin, “NDPsec: Neighbor Discovery Protocol Security Mechanism,” Volume 10, pp. 83650 – 83663, 2022.

2. Lakshmana Rao Kalabarige, Routhu Srinivasa Rao, Ajith Abraham , And Lubna Abdelkareim Gabralla, “Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites,” Volume 10, pp. 79543 - 79552, 2022.

3. Lizhen Tang And Qusay H. Mahmoud, “A Deep Learning-Based Framework for Phishing Website Detection,” Volume 10, pp. 1509 - 1521, 2022.

4. Nguyet Quang Do, Ali Selamat, Ondrej Krejcar Enrique Herrera-Viedma And Hamido Fujita, “Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions,” Volume 10, pp. 36429 - 36463, 2022.

5. Lakshmana Rao Kalabarige, Routhu Srinivasa Rao, Alwyn R. Pais, And Lubna Abdelkareim Gabralla, “A Boosting-Based Hybrid Feature Selection and Multi-Layer Stacked Ensemble LearningModel to Detect Phishing Websites”, Volume 11, pp. 71180 - 71193, 2023.

6. S. W. B. Tan, P. K. Naraharisetti, S. K. Chin, and L. Y. Lee, ``Simple visual-aided automated titration using the Python programming language,"*J. Chem. Educ.*, vol. 97, no. 3, pp. 850_854, Mar. 2020.

7. A.Al-Ani, M. Anbar, A. K. Al-Ani, andI.H.Hasbullah,``DHCPv6Auth:A mechanism to improve DHCPv6 authentication and privacy," *Sadhana,Acad. Proc. Eng. Sci.*, vol. 45, no. 1, Dec. 2020, doi: 10.1007/S12046-019-1244-4.

8. A.K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim,``Matchprevention technique against Denial-of-Service attack on address resolution and duplicate address detection processes in IPv6 link-local network,'' *IEEE Access*, vol. 8, pp. 27122_27138, 2020. Accessed:Mar. 31, 2022.

9. M. Al-Sarem, F. Saeed, A. Alsaeedi, W. Boulila, and T. Al-Hadhrami,``Ensemble methods for instance-based Arabic language authorship attri-bution,'' *IEEE Access*, vol. 8, pp. 17331_17345, 2020.

10. X. Niu, J. Ma, Y. Wang, J. Zhang, H. Chen, and H. Tang, ``A novel decomposition-ensemble learning model based on ensemble empirical mode decomposition and recurrent neural network for landslide displacement prediction,'' *Appl. Sci.*, vol. 11, no. 10, p. 4684, May 2021.

11. L. Tang and Q. H. Mahmoud, ``A survey of machine learning-based solu-tions for phishing website detection,'' Mach. Learn. Knowl. Extraction,vol. 3, no. 3, pp. 672_694, Aug. 2021.

12. Phishing Activity Trends Report 1st Quarter 2021.APWG. Accessed: Oct. 20, 2021.

13. M. A. El-Rashidy, ``A smart model for web phishing detection based on new proposed feature selection technique,'' Menou_a J. Electron.Eng. Res., vol. 30, no. 1, pp. 97_104, Jan. 2021.

14. B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione, and X. Chang, ``A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment,'' *Comput. Commun.*,vol. 175, pp. 47_57, Jul. 2021.

15. E. Gandotra and D. Gupta, ``Improving spoofed website detection usingmachine learning,'' Cybern. Syst., vol. 52, no. 2, pp. 169_190, Oct. 2020.

16. R. Zaimi, M. Ha_di, and M. Lamia, ``Survey paper: Taxonomy of website anti-phishing solutions,'' in Proc. 7th Int. Conf. Social Netw. Anal., Manage. Secur. (SNAMS), Dec. 2020.

17. Odeh, I.Keshta, and E. Abdelfattah, ``Machine LearningTechniques fordetection of website phishing: A review for promises and challenges,'' in Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC),Jan. 2021.

18. L. Tang and Q. H. Mahmoud, ``A survey of machine learning-based solutions for phishing website detection,'' Mach. Learn. Knowl. Extraction, vol. 3, no. 3, pp. 672_694, Aug. 2021

19. E. S. Aung, C. T. Zan, and H. Yamana. A Survey of URL- Based Phishing Detection. Accessed: Mar. 22, 2022.

20. E. Benavides, W. Fuertes, S. Sanchez, and M. Sanchez, ``Classi_cation of phishing attack solutions by employing deep learning techniques: A systematic literature review,'' in Developments and Advances in Defense and Security. Singapore: Springer, 2020.Security. Singapore: Springer, 2020.