Shilling Attack Protection

and Tier-3 Security in Recommender System: E-Commerce Website (ShopNest)

Sumit(152153) | Bablu(152112)
yadavskyst@gmail.com | bphimat2000@gmail.com

UNIVERSITY OF DELHI
Cluster Innovation Centre
University of Delhi

Mentor:
Dr. Anjani Kumar Verma
Assistant Professor

Abstract

In the rapidly evolving domain of e-commerce, recommender systems are pivotal in enhancing user experience and driving sales. However, these systems are vulnerable to shilling attacks, where malicious users inject fake profiles to manipulate recommendations. We presents a comprehensive approach to shilling attack protection and Tier-3 security for ShopNest, an e-commerce platform. We explore the nature of shilling attacks, identifying common patterns and methods to detect and mitigate them using statistical analysis and machine learning techniques. Furthermore, we integrate robust Tier-3 security measures, including multi-factor authentication, role-based access control, data encryption, and real-time anomaly detection systems. Our proposed solution combines advanced data analysis, secure authentication protocols, and continuous monitoring to safeguard the integrity of the recommender system. The result is a resilient framework that not only enhances the accuracy and reliability of product recommendations but also ensures the security and trustworthiness of the e-commerce platform.

Introduction

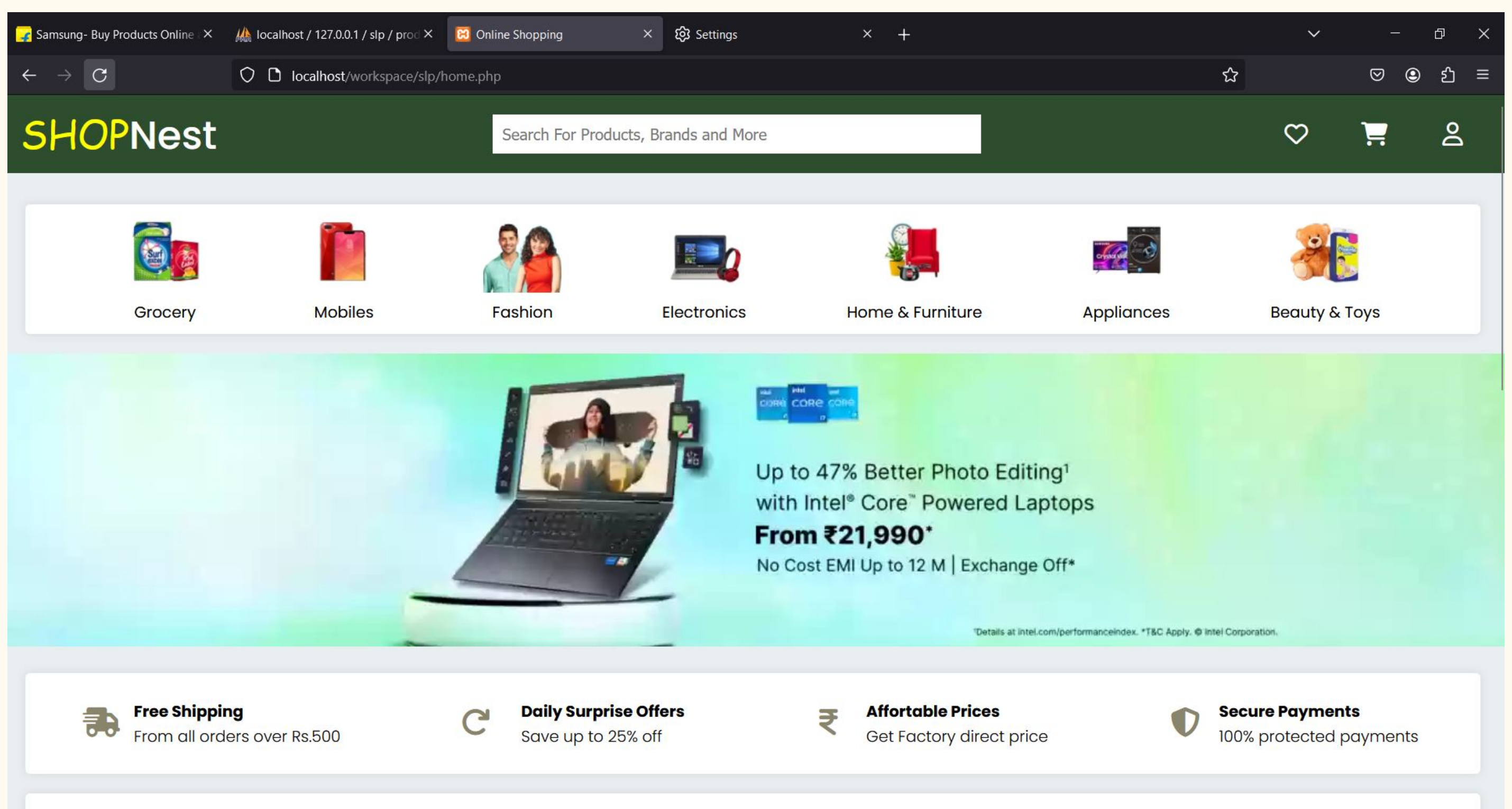
Shilling attacks typically involve push attacks, which artificially inflate the popularity of certain products, and nuke attacks, which aim to damage the reputation of targeted items. Machine learning algorithms play a pivotal role in detecting and mitigating these attacks, as they can analyze large volumes of data to discern genuine user behavior from malicious activity. Traditional methods like profile analysis and behavioral pattern recognition are enhanced by modern machine learning approaches to identify and filter out fraudulent profiles effectively.

Beyond detecting shilling attacks, maintaining Tier-3 security is essential for safeguarding user data and ensuring the overall integrity of the system. Machine learning techniques augment the security measures by providing advanced anomaly detection capabilities, enabling the system to quickly adapt to new attack strategies. This involves implementing multi-factor authentication (MFA) to prevent unauthorized access, role-based access control (RBAC) to limit system permissions, and comprehensive data encryption to protect sensitive information both in transit and at rest. Additionally, continuous monitoring and anomaly detection systems are essential to promptly identify and respond to suspicious activities.

Methodology

The methodology for enhancing security measures on the e-commerce website begins with implementing preliminary preventive measures, including the development of functions and algorithms to combat fake reviews and profiles, along with OTP authentication via PHP Mailer to ensure user registration authenticity. Following this, an AI model is developed by collecting and preprocessing a dataset of both fake and genuine reviews, enabling the detection and filtering of fraudulent content through machine learning techniques. Pending is the integration of Tier-3 security measures, such as password protection, OTP verification, and facial recognition, which involves designing and training a facial recognition model using a dataset of facial images for user authentication. Subsequently, integration and extensive testing are conducted to evaluate the accuracy and effectiveness of the implemented security mechanisms. Further assessment and optimization are pursued to refine the facial recognition model's accuracy and overall security effectiveness, with iterative improvements based on assessment results and user feedback. Finally, upon achieving satisfactory accuracy levels, the AI model and Tier-3 security measures are fully integrated and deployed to the live environment, ensuring ongoing protection against shilling attacks and bolstered user authentication.

Results

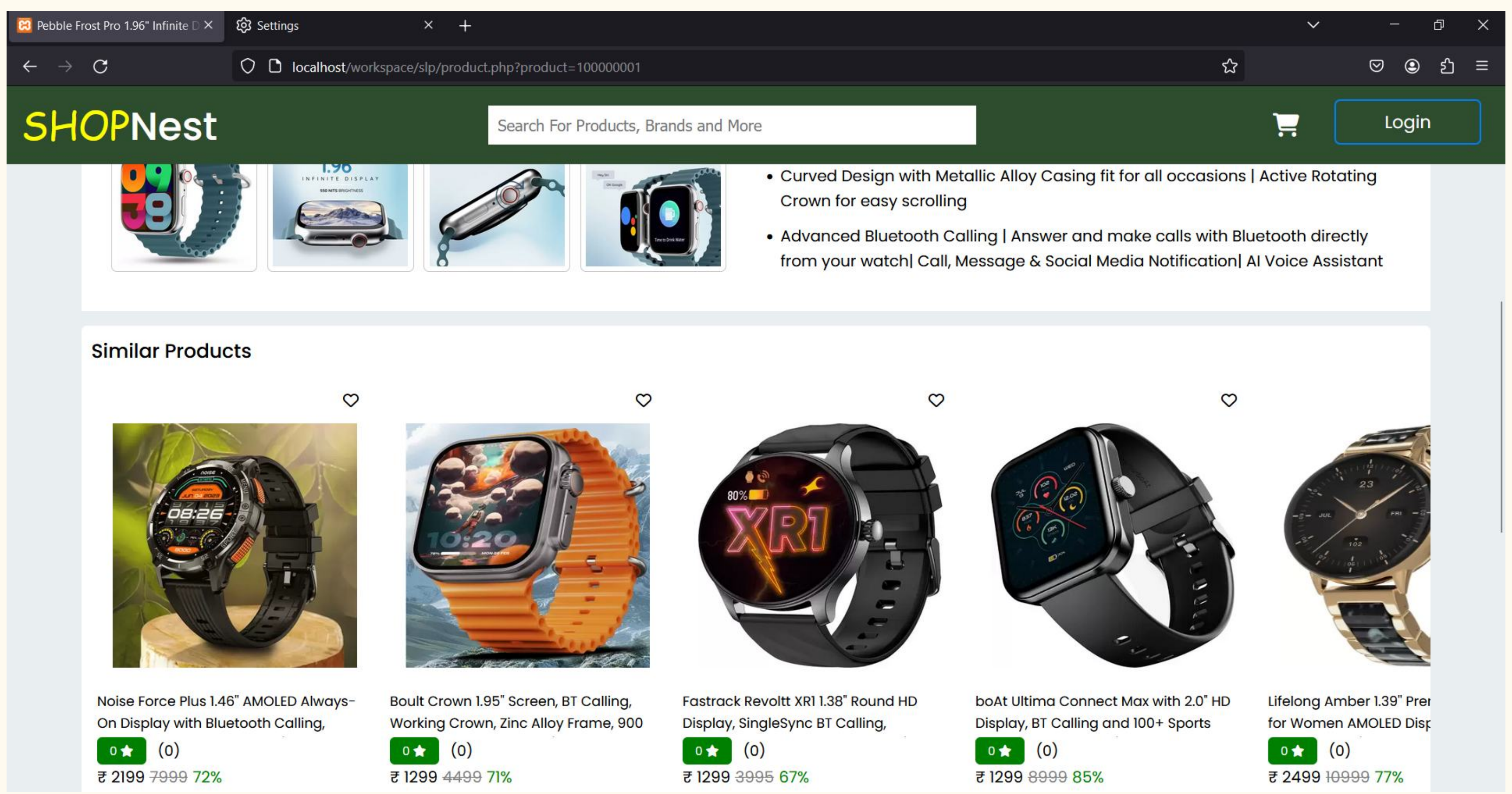

Samsung- Buy Products Online
localhost / 127.0.0.1 / slp / prod
Online Shopping
Settings
localhost/workspace/slp/home.php
SHOPNest
Search For Products, Brands and More
Grocery
Mobiles
Fashion
Electronics
Home & Furniture
Appliances
Beauty & Toys

Up to 47% Better Photo Editing[1] with Intel® Core™ Powered Laptops
From ₹21,990*
No Cost EMI Up to 12 M | Exchange Off*

*Details at intel.com/performanceindex. *T&C Apply. © Intel Corporation.

Free Shipping From all orders over Rs.500
Daily Surprise Offers Save up to 25% off
Affortable Prices Get Factory direct price
Secure Payments 100% protected payments

Fig 1: E-Commerce Website


Pebble Frost Pro 1.96" Infinite D
Settings
localhost/workspace/slp/product.php?product=100000001
SHOPNest
Search For Products, Brands and More
Login
1.96
INFINITE DISPLAY
Similar Products

- Curved Design with Metallic Alloy Casing fit for all occasions | Active Rotating Crown for easy scrolling
- Advanced Bluetooth Calling | Answer and make calls with Bluetooth directly from your watch| Call, Message & Social Media Notification| AI Voice Assistant

Noise Force Plus 1.46" AMOLED Always-On Display with Bluetooth Calling,
0 ★ (0)
₹ 2199 ~~7999~~ 72%

Boult Crown 1.95" Screen, BT Calling, Working Crown, Zinc Alloy Frame, 900
0 ★ (0)
₹ 1299 ~~4499~~ 71%

Fastrack Revoltt XR1 1.38" Round HD Display, SingleSync BT Calling,
0 ★ (0)
₹ 1299 ~~3995~~ 67%

boAt Ultima Connect Max with 2.0" HD Display, BT Calling and 100+ Sports
0 ★ (0)
₹ 1299 ~~8999~~ 85%

Lifelong Amber 1.39" Pre for Women AMOLED Disp
0 ★ (0)
₹ 2499 ~~10999~~ 77%

Fig 2:Recommender System

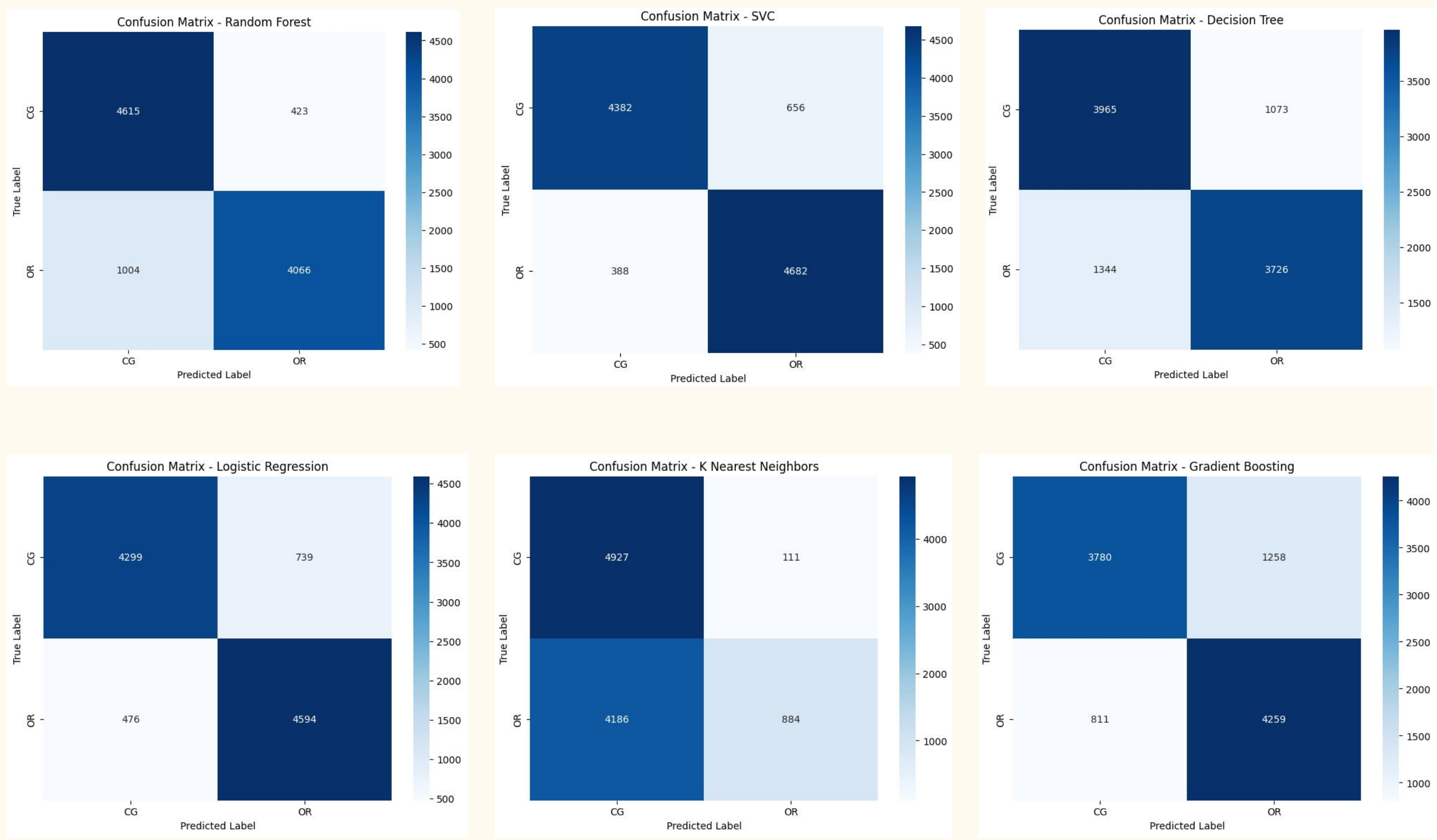


Fig 3: Confusion matrix of different models used to Train the Fake Review dataset

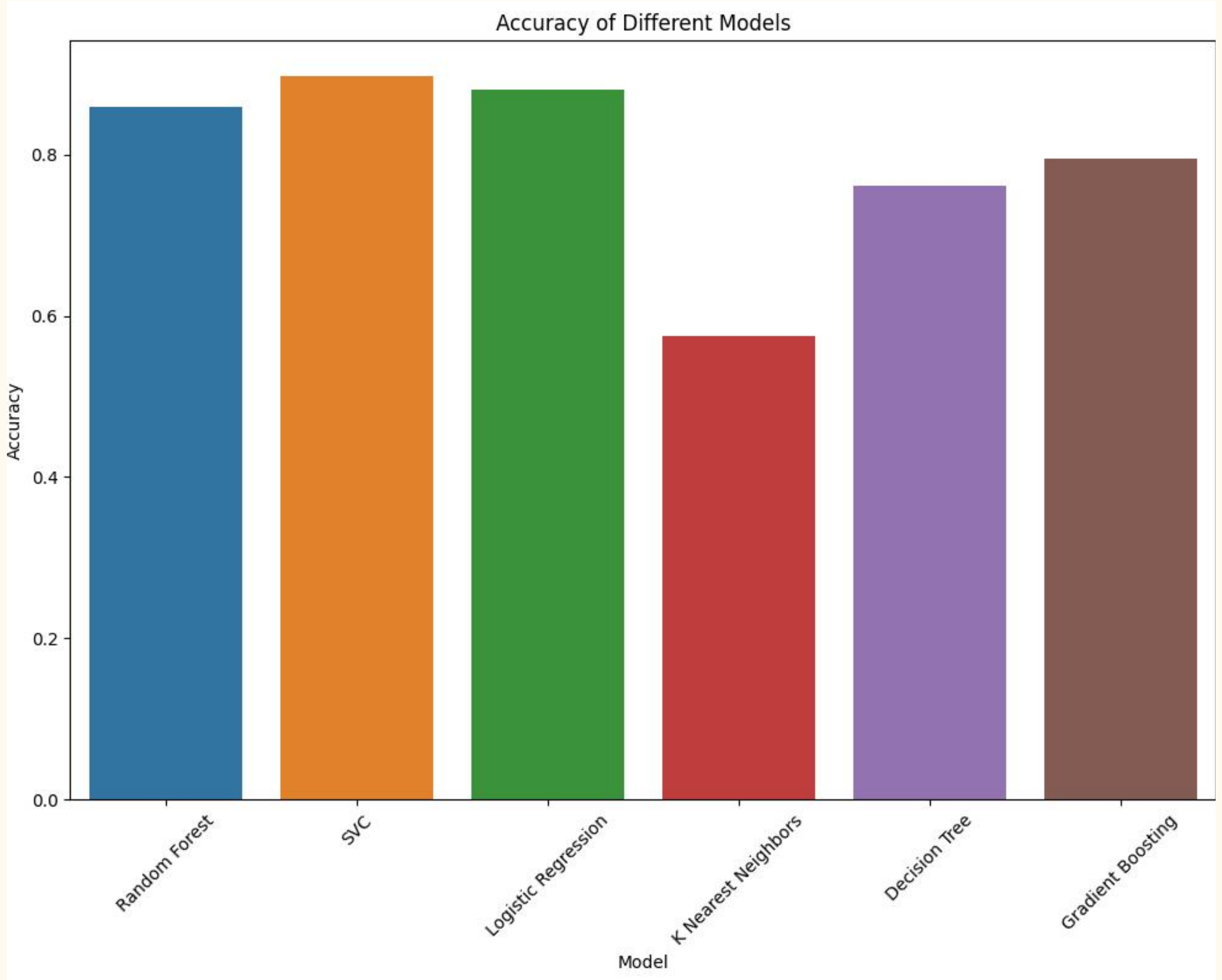


Fig 4: Accuracy Of Different Models

Technologies Used

php, MySQL, jupyter, Apache, HTML, CSS, JS, PHPMailer, K, AJAX

References

- Gunes, I., Kaleli, C., Bilge, A., & Polat, H. (2014). Shilling attacks against recommender systems: a comprehensive survey. Artificial Intelligence Review, 42, 767-799.
- Si, M., & Li, Q. (2020). Shilling attacks against collaborative recommender systems: a review. Artificial Intelligence Review, 53, 291-319.
- Bilge, A., Ozdemir, Z., & Polat, H. (2014). A novel shilling attack detection method. Procedia Computer Science, 31, 165-174.