IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# BRANDGUARD: AI-DRIVEN THREAT INTELLIGENCE WITH SENTIMENT ANALYSIS

**[1]Anu C, [2]Muhammed Hadhif Manoly, [3]Aysha Shama Musamil, [4]Anand K K, [5]Afnas C P**

[1]Asst. Professor, [2]Student, [3]Student, [4]Student, [5]Student
Department of Computer Science and Engineering
St. Thomas College of Engineering and Technology, Kannur, Kerala, India

***Abstract :*** Brands today face serious risks from fake websites, counterfeit products, and negative reviews that can harm their reputation. Traditional AI methods often struggle to detect these threats effectively. BRANDGUARD is an AI-powered system designed to tackle this issue. It continuously scans the internet to find fraudulent websites, monitors online stores for counterfeit products and detects negative customer reviews that could impact a brand's image. By combining real-time monitoring, image analysis, and sentiment detection, BRANDGUARD helps brands quickly identify and respond to potential threats, ensuring their reputation and customer trust remain protected.

***Index Terms*** **- Threat Intelligence, Fake Website Detection, Counterfeit Product Detection, Negative Review Detection.**

## I. INTRODUCTION

In today's fast-paced and continuously evolving digital environment, brands are increasingly exposed to a variety of cyber threats that can significantly damage their reputation and undermine consumer trust. The widespread availability of the internet has led to a dramatic rise in fraudulent activities, including targeted fake websites that mimic legitimate brands, the sale of counterfeit or substandard products, and the spread of misleading reviews. These threats not only cause financial losses for businesses but also erode customer confidence—a recovery from which can take years.

To address these challenges, we introduce BRANDGUARD, an AI-Driven Threat Intelligence platform designed to proactively safeguard brand integrity through computer vision-based detection of counterfeit websites and fake products, along with advanced sentiment analysis to monitor public perception. Unlike conventional methods, BRANDGUARD leverages artificial intelligence to detect fake websites, verify product authenticity using visual analysis, and identify negative sentiment in customer reviews. This pronged approach enables brands to swiftly respond to emerging threats while effectively managing their reputation in the ever-changing digital landscape. By integrating AI-powered visual analysis, logo detection, and sentiment intelligence, BRANDGUARD provides a comprehensive and automated defense system against brand exploitation.

## II. PROBLEM DEFINITION

In today's digital landscape, brands face growing threats from fraudulent websites, counterfeit products, and misleading reviews, putting their reputation and customer trust at risk. Cybercriminals create phishing websites that closely mimic legitimate brands using similar domain names and designs, deceiving customers into purchasing fake clothing or sharing sensitive data. Counterfeit products misuse brand logos, leading to poor-quality purchases that damage the original brand's credibility.

Additionally, manipulated online reviews can distort public perception, influencing buyers and harming trust. Traditional brand protection methods relying on manual monitoring and reactive measures are ineffective against these evolving threats. To counter this, BRANDGUARD employs an AI-driven approach integrating web monitoring, computer vision, and NLP for real-time detection and mitigation. It uses Levenshtein Distance and Sequence Matcher algorithms to detect phishing websites, while SIFT-based logo verification identifies counterfeit products. Additionally, BERTbased sentiment analysis flags harmful reviews. By automating threat detection, BRANDGUARD provides brands with a comprehensive defense system to safeguard their reputation and maintain consumer trust in an increasingly competitive digital world.

## III. EXISTING SYSTEM

The system is an AI-powered automated framework designed to detect phishing attacks targeting banking, ecommerce, and corporate websites. Unlike traditional methods that analyze URLs or text, this system focuses on visual elements such as layout, logos, fonts, and color schemes, which are harder for attackers to replicate. Using computer vision and AI, it compares websites against a database of trusted sites, detecting subtle inconsistencies like misaligned elements or low-quality logos. The system operates in real time, autonomously analyzing suspicious websites and providing instant alerts. Additionally, it can integrate with machine learning models and behavioral analytics for enhanced security. This multilayered approach ensures high accuracy, faster detection and better protection against phishing threats.

## IV. RELATED WORKS

Before starting a new study, a literature review provides a comprehensive understanding of existing research, helping to explore current methodologies, challenges, and solutions relevant to the field. For our project, we analyzed four research papers that align with brand protection and cyber defense. The study on Detection of Fake Online Reviews using Machine Learning [2] focuses on identifying fraudulent reviews that impact brand reputation, while Real-Time Detection of Fake Shops through Machine Learning [11] discusses methods for detecting counterfeit e-commerce stores. Additionally, the research on Detecting Targeted Phishing Websites for Brand Protection and Cyber Defence using Computer Vision [1] explores AI-based phishing website detection. These studies provided valuable insights into fake review detection, counterfeit product identification, and phishing prevention, forming the foundation for developing BrandGuard, a comprehensive AI-driven brand protection system.

### *A. Detection of Fake Online Reviews using Machine Learning*

The model discussed in the paper uses a heterogeneous graph transformer to detect fake online reviews by analyzing relationships between customers, products, and reviews. It improves accuracy by integrating user preferences, content analysis, and image-based features, adapting to new data while minimizing overfitting. The workflow begins with data preprocessing to clean and normalize reviews, followed by feature extraction to identify sentiment indicators, ratings, and review patterns. A balanced sampling strategy prevents bias, ensuring fair classification. The model is then trained using graph-based embeddings and classified with supervised algorithms like SVM, evaluated through accuracy and precision metrics. To stay effective, it incorporates continuous learning, adapting to evolving fraudulent patterns over time [2].

### *B. Real-Time Detection of Fake Shops through Machine Learning*

The system uses machine learning (XGBoost, Random Forest) to analyze website source code and detect fraudulent online shops. It extracts HTML, JavaScript, and structural patterns to classify websites and improves through real-time data analysis.A Heterogeneous Graph Transformer Model detects fake online reviews by analyzing relationships between users, products, and reviews. It integrates with classification algorithms for accurate fraud detection and adapts to evolving tactics.The system assigns risk scores to websites, monitors domains, and provides an expert dashboard for fraud prevention. A browser plugin alerts users in real-time, ensuring continuous protection against fake e-commerce sites.[11]

### *C. Detecting Targeted Phishing Websites for Brand Protection and Cyber Defence using Computer Vision*

The system is an automated framework designed to detect phishing attacks targeting banking, e-commerce, and corporate websites. It prevents cybercriminals from deceiving users into revealing sensitive data by identifying fraudulent website copies. Unlike traditional phishing detection methods that rely on URL and text analysis, this system uses computer vision and AI to analyze visual elements such as layout, colors, fonts, and logos. By detecting subtle design inconsistencies, it accurately distinguishes between real and fake websites. AI algorithms enhance detection by comparing websites against a trusted database and continuously learning from phishing trends. The system operates autonomously, providing real-time analysis and instant alerts without manual intervention. It integrates with machine learning models and behavioral analytics for enhanced security, offering a multi-layered approach to phishing detection. This advanced AI-powered solution provides faster, more accurate, and automated protection for high-value websites [1].

TABLE I. LITERATURE SURVEY TABLE

| PAPER | DESCRIPTION | AUTHOR |
|---|---|---|
| Detection of Fake Online Reviews Using Machine Learning. | Utilizes supervised learning models (e.g., SVM, Naive Bayes) to classify reviews as fake or genuine | C. Silpa, P Prasanth, S Sowmya, Y Bhumika, C H Surya Pavan, M Naveed |
| Real-Time Detection of Fake-Shops through Machine Learning | A machine learning approach to classify fake online shops based on source code similarity. | Louise Beltzung, Andrew Lindley, Olivia Dinica, Nadin Hermann, Raphaela Lindner |
| Detecting Targeted Phishing Websites for Brand Protection and Cyber Defence Using Computer Vision | Utilizes a multi-module system for detection, acquisition, evaluation, and response to phishing threats | Carlos Pires, Jose´ Borges |

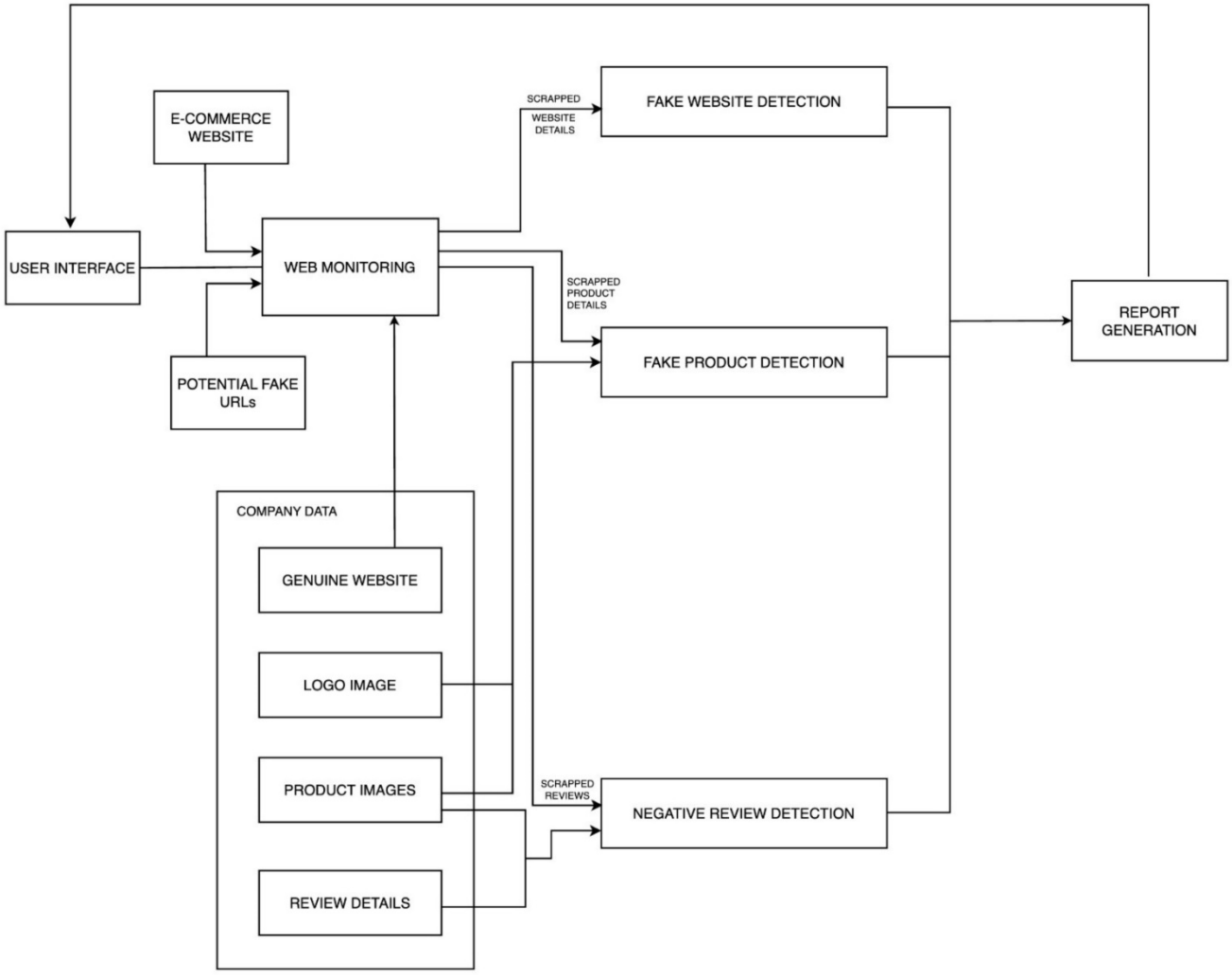
## V. PROPOSED SYSTEM

BRANDGUARD is an AI-powered threat detection system designed to safeguard brands from online risks such as fraudulent websites, counterfeit products and negative reviews. It uses domain analysis to identify fake websites mimicking official brands, computer vision to detect counterfeit products by analyzing product images and sentiment analysis to track negative customer feedback. By automating these processes, BRANDGUARD provides real-time insights, allowing brands to quickly respond to threats, preserve their identity and maintain consumer trust in an increasingly digital marketplace.

### *A. Architecture*

The architecture diagram in the figure 1 represents the workflow of the BRANDGUARD system. It integrates key components to detect and mitigate online threats in real time. The user interface serves as a dashboard for monitoring fake websites, counterfeit products, and negative reviews. ClickMart, the e-commerce platform, is monitored for fraudulent listings. Web monitoring automates data collection by scraping fake URLs, product images, and reviews. Fake website detection analyzes site structure and content using computer vision, while fake product detection extracts and compares product logos to detect counterfeits. Negative review detection applies sentiment analysis to identify harmful feedback. Company data stores genuine brand assets for accurate comparisons, and report generation compiles detection results for immediate action. A real-time alert mechanism ensures that brands are notified immediately when a potential threat is detected. The system continuously learns from new data, improving detection accuracy over time. By integrating AI-driven analysis and automation, BRANDGUARD enhances brand security and minimizes the risk of digital fraud.

Figure 1. Architecture Diagram




1) User Interface (UI): Acts as the central dashboard where brands monitor fake websites, counterfeit products, and negative reviews, enabling quick decision-making.

2) E-Commerce Website (ClickMart): A marketplace for multiple brands, monitored to detect fraudulent listings from third-party sellers.

3) Web Monitoring: Automates data collection by scraping fake URLs, product images, and reviews from ClickMart, keeping the system updated.

4) Fake Website Detection: Analyzes website structure, layout, and logos using computer vision to identify phishing attempts.

5) Fake Product Detection: Extracts and compares logos and product images with authentic brand data to detect counterfeit listings.

6) Negative Review Detection: Applies sentiment analysis to identify harmful feedback, spam, or malicious reviews affecting brand reputation.

7) Company Data: Stores genuine brand assets, including website structures, logos, and product details, ensuring accurate threat detection.

8) Report Generation: Compiles detection results into realtime reports, enabling brands to take immediate action against fraudulent activities.

### *B. Creation and Hosting of Brand-Related Websites and Web Monitoring for Fake Websites*

For the purpose of demonstrating the project, a clothing brand named Heliix was created, and its official website was developed and hosted. Additionally, a fake website was intentionally created and deployed to simulate brand impersonation attempts. This module ensures the secure establishment and monitoring of brand-owned websites while actively scanning the web for fraudulent domains that attempt to mimic the brand. The detection of fake websites is carried out using domain similarity analysis, where Levenshtein Distance is applied to measure the similarity between a suspicious domain and the official website. A high similarity score indicates a potential phishing attempt.

Additionally, Sequence Matcher (Longest Common Subsequence - LCS) is used to analyze and compare textual content across websites, helping identify cases where counterfeit sites copy brand-related content. A real-time monitoring system is integrated, which continuously scans the web at scheduled intervals to identify newly hosted fraudulent websites. When both domain similarity and content similarity exceed a predefined threshold, the system classifies the website as potentially fake and generates an alert. These proactive detection mechanisms allow businesses to mitigate risks associated with phishing attacks, online fraud, and brand identity theft. By securing the brand's digital presence, this module plays a crucial role in protecting both businesses and consumers from deceptive online threats.

### *C. Real-Time Fake Product Detection on E-Commerce Websites*

To illustrate the implementation of this module, an ecommerce platform named ClickMart was developed, offering a wide range of clothing and non-clothing products from multiple brands. Within this platform, unauthorized sellers may attempt to list counterfeit products under well-known brand names, such as Heliix. The system is designed to automatically scrape product images and details from ClickMart and crosscheck them against a dataset of genuine brand products to identify fraudulent listings.

A MobileNetV2-based deep learning model is employed to classify whether an image belongs to a clothing product. Once an item is identified as clothing, Scale-Invariant Feature Transform (SIFT) is applied to extract key visual features from the image, and the Brute-Force Matcher (BFMatcher) is used to compare the extracted features with authentic brand product images. If the similarity score falls below a predefined threshold, the product is flagged as counterfeit.

By implementing real-time product verification, the system ensures that counterfeit products do not mislead consumers and harm the brand's reputation. This automated detection mechanism helps e-commerce platforms like ClickMart combat unauthorized resellers and maintain product authenticity. Through the integration of advanced image recognition and deep learning techniques, this module provides a scalable, efficient, and AI-driven approach to counterfeit product mitigation.

### *D. Sentiment Analysis of Product Reviews*

Customer reviews serve as a vital source of feedback, reflecting consumer satisfaction and product authenticity. To assess customer perception, reviews from ClickMart, particularly for Heliix products, were analyzed using sentiment analysis techniques. This module utilizes DistilBERT, an advanced Natural Language Processing (NLP) model, to classify reviews into positive or negative sentiment categories.

The review text undergoes preprocessing and tokenization using DistilBert Tokenizer, converting it into a machinereadable format for efficient analysis. The Softmax classification technique is then applied to determine the sentiment polarity of each review. If a review is classified as negative, it is logged and displayed for further evaluation.

This module plays a critical role in helping brands identify common customer complaints, detect dissatisfaction trends, and address potential issues related to product quality or service. By automating opinion mining and sentiment detection, businesses can efficiently monitor their brand reputation, respond proactively to customer concerns, and enhance consumer trust. The ability to analyze large volumes of customer feedback in real-time provides a data-driven approach to improving brand perception and product satisfaction.

### *E. Creation of E-Commerce Website and User Interface and Integration.*

An e-commerce site named ClickMart was developed to facilitate the sale of clothing and non-clothing products from various brands while incorporating mechanisms to detect fake products and negative reviews of the Heliix brand. The platform was designed to provide a seamless shopping experience while actively monitoring product listings for authenticity using computer vision-based fake product detection techniques. This ensures that counterfeit products are identified in real time, preventing unauthorized sellers from misleading consumers.

To provide centralized brand monitoring, the BrandGuard user interface was developed as a comprehensive dashboard, integrating all detection modules into a single platform. A login system was implemented for registered brands, enabling them to access a real-time monitoring dashboard where critical insights related to brand protection are displayed. The system actively detects and lists fake websites attempting to impersonate the brand, showing fraudulent site URLs along with their domain similarity scores. Additionally, it monitors fake product listings, displaying counterfeit product names and seller URLs. Sentiment analysis is also integrated into the dashboard, providing an overview of customer reviews of Heliix products, with AI-based detection of negative feedback.

## VI. RESULT

The BRANDGUARD system has been extensively tested and evaluated to determine its effectiveness in detecting fake websites, counterfeit products, and negative customer reviews. This section presents the analysis of the results obtained from various testing and evaluation procedures, focusing on accuracy, performance, and real-time detection efficiency.

### *A. Dashboard for BrandGuard*

The figure 2 presents the dashboard serves as a centralized interface for brands to monitor and manage online threats in real time. It provides a comprehensive view of detected fake websites, counterfeit products, and negative reviews, allowing brands to take immediate action. The dashboard is designed for ease of use, displaying key insights such as flagged phishing domains, unauthorized product listings, and sentiment analysis results. With automated alerts and real-time updates, it ensures quick decision-making and efficient threat mitigation. By integrating multiple detection modules into a single platform, the BRANDGUARD dashboard enhances brand security and streamlines digital risk management.

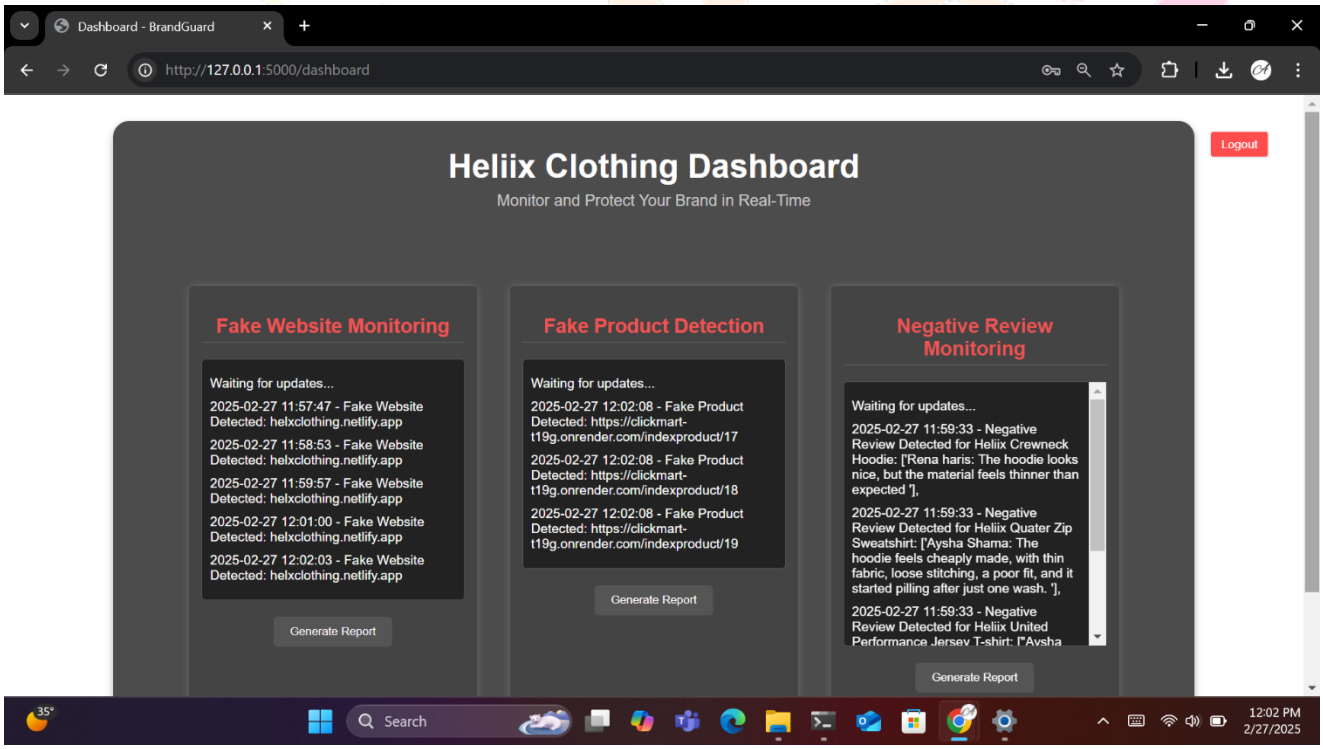



Figure. 2. Dashboard for BrandGuard

The fake website monitoring module continuously scans for fraudulent domains impersonating Heliix Clothing, instantly updating the interface and allowing users to generate detailed reports. The fake product detection module monitors unauthorized listings on online marketplaces, using image verification techniques to identify counterfeits and providing real-time updates. The negative review monitoring module applies NLP to detect negative reviews.

### *B. Genuine Website*

The Heliix Clothing original brand page, shown in Figure 3, is a visually appealing and user-friendly e-commerce platform showcasing a diverse collection of stylish and high-quality apparel. The homepage features a banner image prominently displaying the brand's identity, creating an engaging first impression for visitors.

The core of the website is the products grid, which elegantly organizes Heliix Clothing's collection into multiple rows, displaying items such as t-shirts, hoodies, sweatshirts, and polo shirts. Each product card contains a high-quality image, product name, and price, with hover effects that add a touch of interactivity. Clicking on a product redirects users to a dedicated product details page.

The website is designed with a modern, responsive layout, ensuring seamless navigation across different screen sizes. The color scheme blends deep blues, bold accents, and neutral backgrounds, creating a clean and professional look. A footer section provides essential contact details, including an email address, phone number, and physical location, ensuring accessibility for customer inquirie

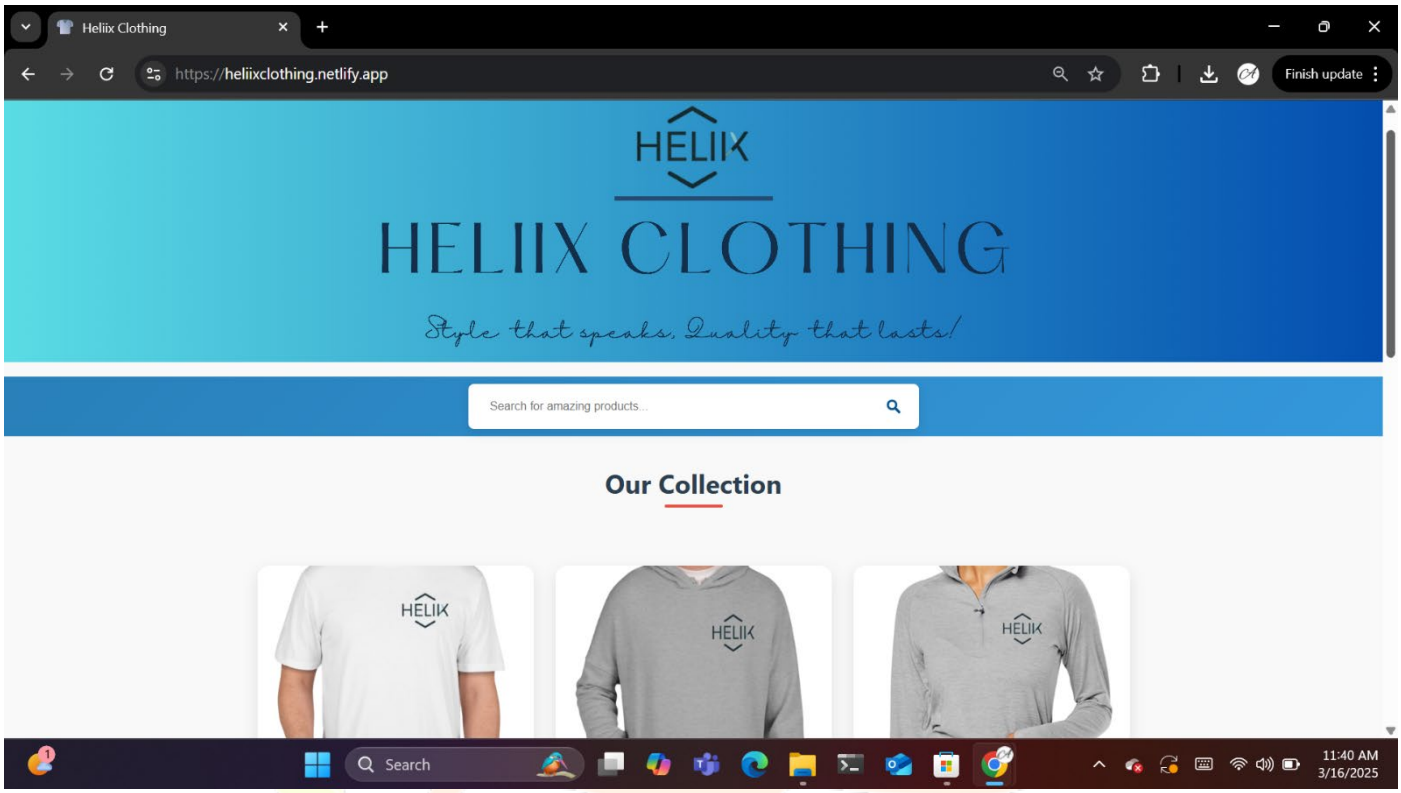



Figure. 3. Heliix Clothing Website

### *C. Fake Website*

The fake website "Helx Clothing" closely mimics the genuine Heliix Clothing website in terms of design, layout, and overall structure, making it deceptive to unsuspecting customers. Both websites feature a banner image, a search bar, and a products grid showcasing various clothing items. As shown in Figure 4, the color scheme, fonts, and card-style product display are almost identical to the original site, making it difficult to distinguish at first glance.

However, a key giveaway is the slightly altered brand name, with "Helx" replacing "Heliix," a common tactic used in phishing and counterfeit scams to mislead users. While the layout and visuals appear legitimate, the domain name, contact details, or backend payment methods may differ, potentially leading customers to fraudulent transactions. The product images and descriptions are likely copied from the real website, giving the illusion of authenticity, but there may be pricing inconsistencies or missing security features such as SSL encryption and secure payment gateways. These minor but crucial discrepancies indicate that the Helx Clothing website is a fraudulent imitation designed to exploit Heliix Clothing's brand reputation. Customers should always verify domain names, look for official security certificates, and compare contact details with the authentic site to avoid falling victim to such scams

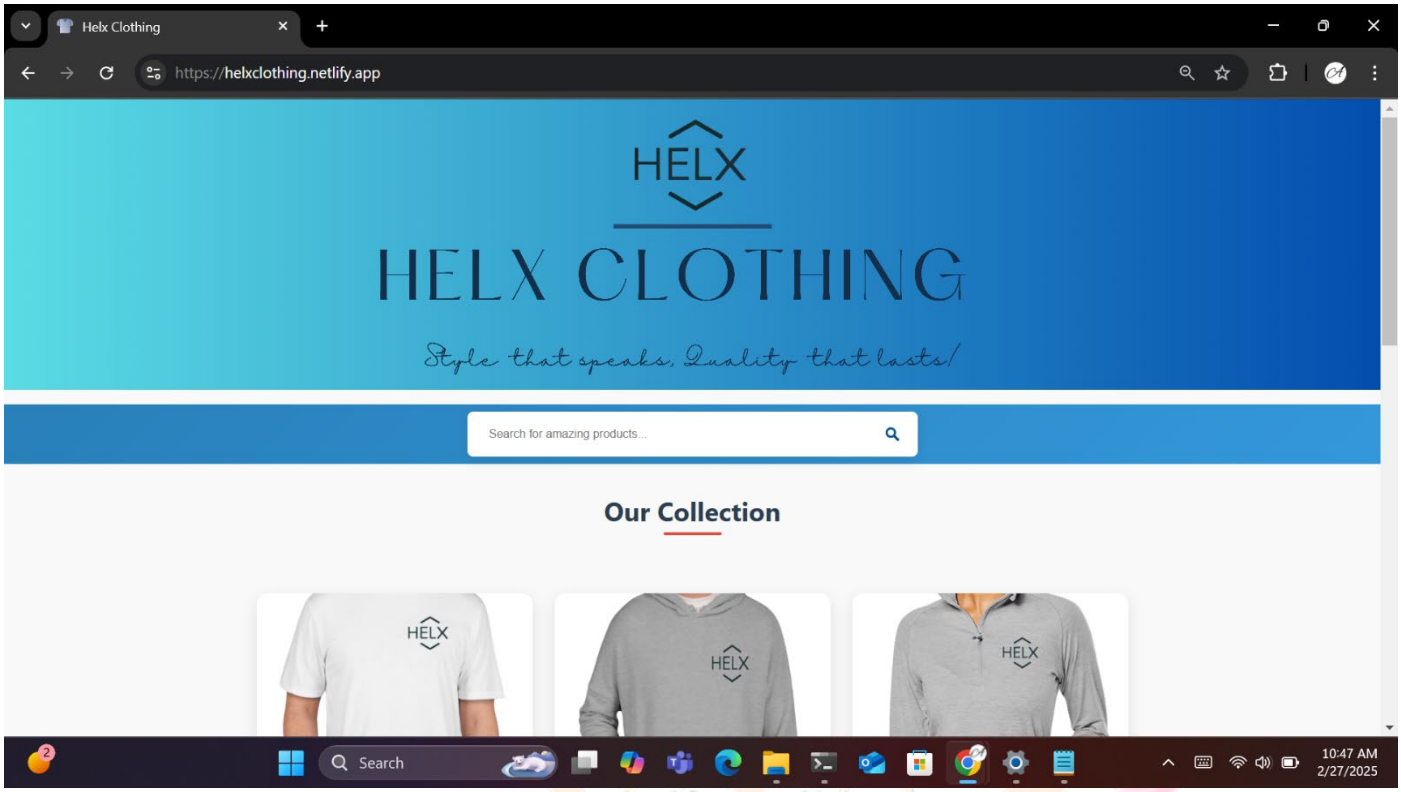



Figure. 4. Helx Clothing Website

### *D. E-commerce Website*

The ClickMart e-commerce website's home page as shown in Figure 5, serves as the primary marketplace where real-time counterfeit product detection takes place through web scraping. The platform features a dynamic product listing section, where multiple sellers can showcase their products, making it a potential target for counterfeit listings. The real-time monitoring system integrated into BrandGuard continuously scrapes this page to detect counterfeit products listed in this website.

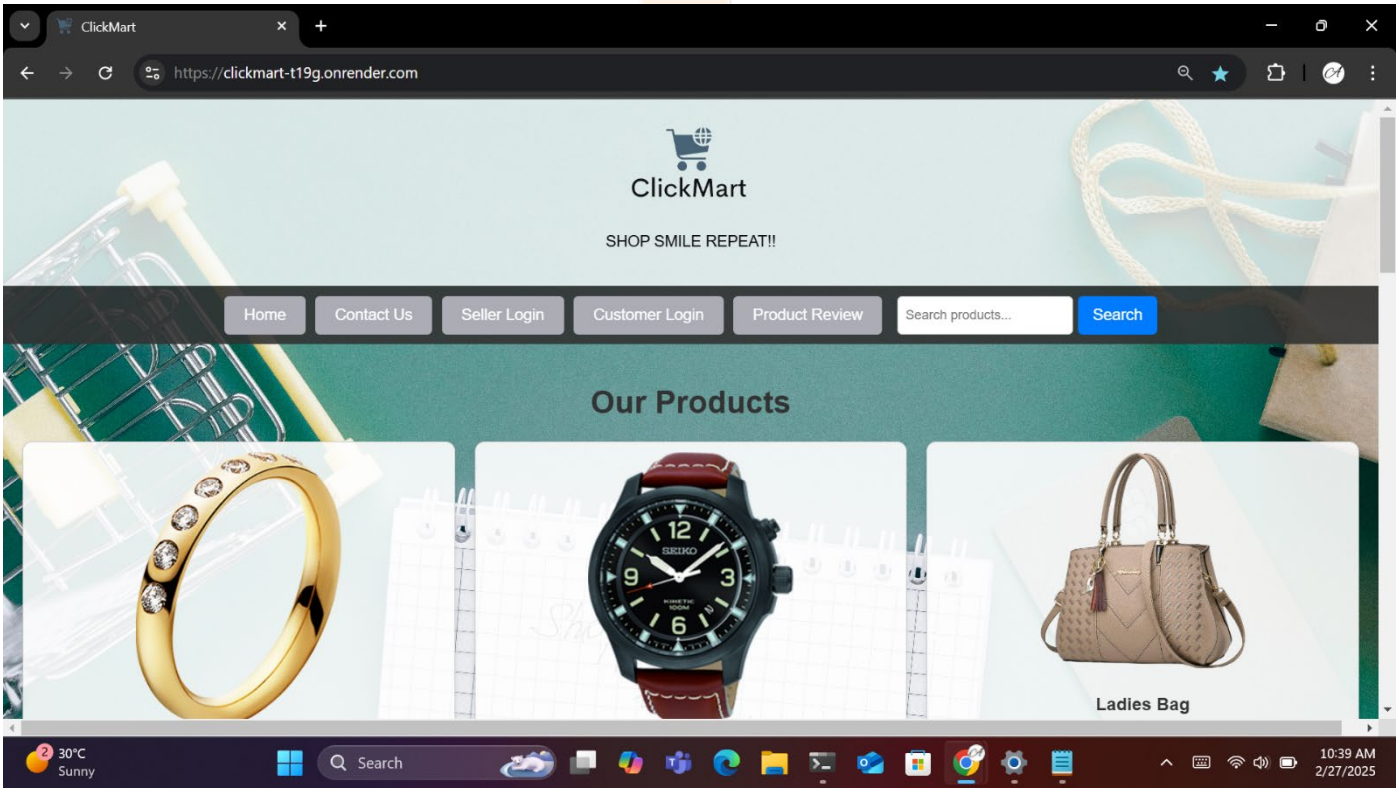



Figure. 5. ClickMart E-commerce Website

The Product Reviews page on ClickMart, as shown in Figure 6, is a crucial section where real-time sentiment analysis is conducted through web scraping to detect negative reviews of Heliix Clothing products. The page features a grid layout displaying various products along with customer-submitted reviews, making it an ideal source for monitoring customer feedback.

The BrandGuard system continuously scrapes this page to extract product names, customer reviews, and reviewer details. Once the reviews are collected, NLP techniques, specifically DistilBERT, are used to analyze the sentiment of each review. The system is designed to identify subtle negativity in comments, even those that seem neutral but imply dissatisfaction. If a negative review is detected, the system automatically logs it and updates the BrandGuard dashboard, ensuring that brand receive real-time alerts about potential customer dissatisfaction.

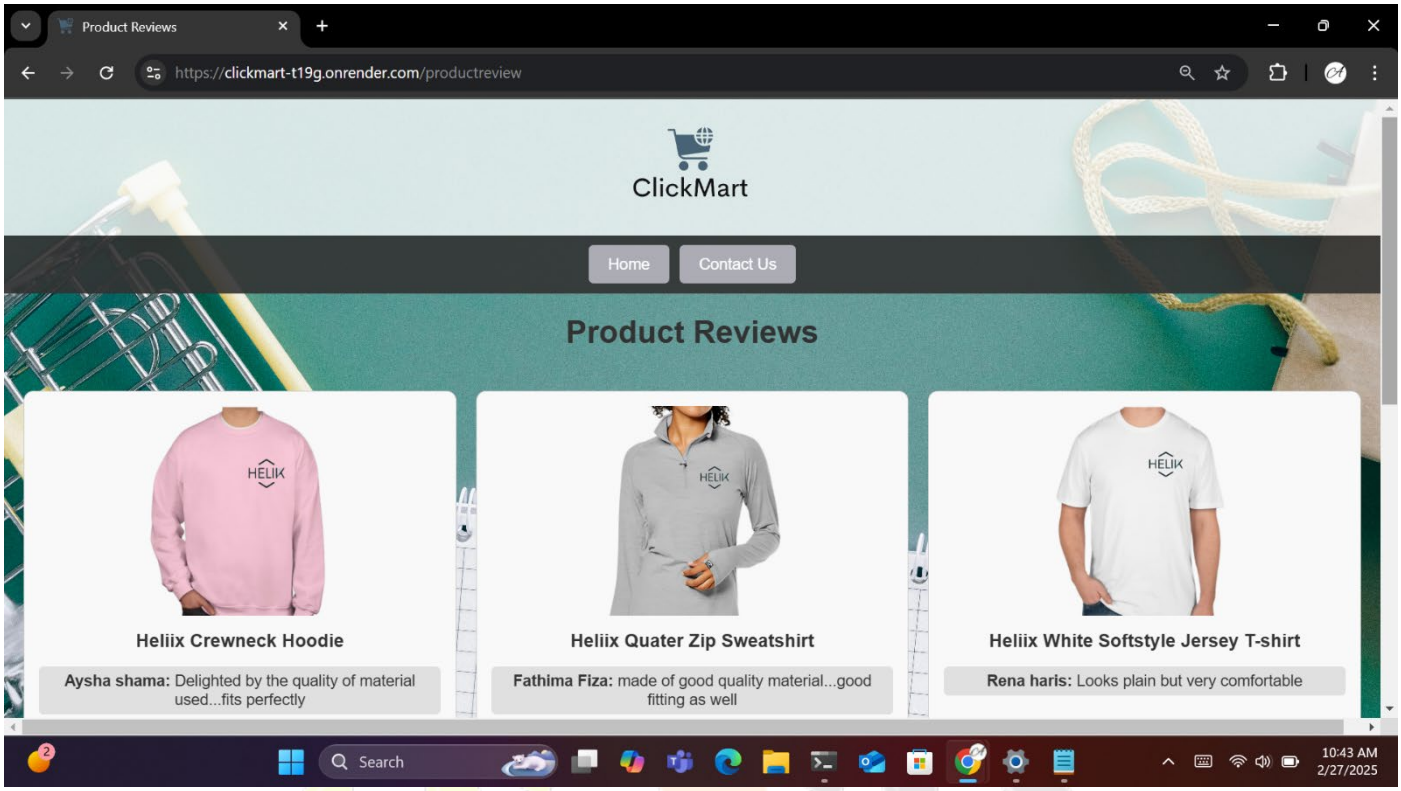



Figure 6. Review Page of E-commerce Website

### *E. Fake Website Detection Performance*

The table II presents precision, recall, and F1-score for identifying genuine and fake websites. The model achieved 100% recall for genuine websites, ensuring all legitimate sites were correctly identified. Additionally, the precision for fake websites was 1.00, meaning every website classified as fake was indeed fraudulent. It effectively analyzed a total support of 7 websites (3 genuine and 4 fake), demonstrating its capability to assess multiple domains.

TABLE II. FAKE WEBSITE DETECTION PERFORMANCE

| Category | Precision | Recall | F1- Score | Support |
|---|---|---|---|---|
| Genuine Website | 0.75 | 1.00 | 0.86 | 3 |
| Fake Website | 1.00 | 0.75 | 0.86 | 4 |

### *F. Fake Product Detection Performance*

The table III presents precision, recall, and F1-score for identifying genuine and fake products. The detection system maintained 0.75 precision and recall for genuine products, showing consistency in identifying authentic listings. With a support of 4 genuine products, the model ensures a solid reference for counterfeit detection, contributing to reliable classification

TABLE III. FAKE PRODUCT DETECTION PERFORMANCE

| Category | Precision | Recall | F1- Score | Support |
|---|---|---|---|---|
| Genuine Product | 0.75 | 1.00 | 0.86 | 4 |
| Fake Product | 0.67 | 0.67 | 0.67 | 3 |

### *G. Sentiment Analysis Performance*

The table IV presents precision, recall, and F1-score for identifying positive and negative reviews. The system achieved 100% recall for positive reviews, ensuring no actual positive feedback was misclassified. Additionally, the precision for negative reviews was

1.00, meaning all detected negative reviews were truly negative. The system also processed a support of 3 positive and 4 negative reviews, showcasing its ability to handle diverse customer feedback efficiently.

TABLE IV. FAKE PRODUCT DETECTION PERFORMANCE

| Category | Precision | Recall | F1- Score | Support |
|---|---|---|---|---|
| Positive Review | 0.75 | 1.00 | 0.86 | 3 |
| Negative Review | 1.00 | 0.75 | 0.86 | 4 |

## VII. CONCLUSION

The BRANDGUARD system provides a comprehensive approach to identifying fake websites, detecting counterfeit products, and analyzing customer sentiment, helping brands maintain their authenticity and credibility in the digital marketplace. In an era where online platforms are widely used for commerce and consumer engagement, fraudulent activities such as brand impersonation, unauthorized product listings, and negative misinformation pose significant challenges. This system ensures continuous monitoring and automated detection, allowing brands to take timely actions against online threats.

At the core of BRANDGUARD is the integration of advanced detection algorithms that enable real-time analysis of website domains, product images, and customer reviews. The fake website detection module utilizes Levenshtein Distance and SequenceMatcher to identify fraudulent domains and duplicated content, ensuring that brands can detect impersonation attempts before they cause reputational damage. The fake product detection module leverages MobileNetV2 and SIFT-based feature extraction to compare product images against a database of genuine brand products, flagging counterfeit listings on e-commerce platforms. Additionally, the sentiment analysis module employs DistilBERT to classify customer reviews, identifying negative feedback that could indicate product dissatisfaction or misleading product claims. By combining these modules into a single user-friendly dashboard, the system provides real-time insights into online brand-related risks, allowing brands to monitor, analyze, and act upon potential threats efficiently.

## REFERENCES


**[1]** C. Pires and J. Borges,"Detecting Targeted Phishing Websites for Brand Protection and Cyber Defence Using Computer Vision",2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Rome, Italy, 2023.

**[2]** C. Silpa, P. Prasanth, S. Sowmya, Y. Bhumika, C. H. S. Pavan and M. Naveed"Detection of Fake Online Reviews by using Machine Learning",2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 71-77.

**[3]** B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras,"Mitigation strategies against the phishing attacks: A systematic literature review",Computers Security, vol. 132, Sep. 2023.

**[4]** S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld, and A. Laszka,"Survey and Taxonomy of Adversarial Reconnaissance Techniques",ACM Comput. Surv., vol. 55, no. 6, pp. 1–38, Jul. 2023.

**[5]** S. Khandelwal and R. Das, "Phishing Detection Using Computer Vision",Computer Networks and Inventive Communication Technologies, 2022.

**[6]** J. Zhou, Y. -F. Liu and H. -L. Sun, "A Reputation Ranking Method based on Rating Pattems and Rating Deviation", 2022 5th International Conference on Data Science and Information Technology (DSIT), pp. 1-6, 2022.

**[7]** C. G. Harris, "Combining Linguistic and Behavioral Clues to Detect Spam in Online Reviews", 2022 IEEE International Conference on e-Business Engineering (ICEBE), pp. 38-44, 2022.

**[8]** P. Rathore, J. Soni, N. Prabakar, M. Palaniswami and P. Santi, "Identifying Groups of Fake Reviewers Using a Semisupervised Approach", IEEE Transactions on Computational Social Systems, vol. 8, no. 6, pp. 1369-1378, Dec. 2021.

**[9]** S. Tang, L. Jin and F. Cheng, "Fraud Detection in Online Product Review Systems via Heterogeneous Graph Transformer",IEEE Access, vol. 9, pp. 167364-167373, 2021

**[10]** B. Conlin and U. Ruhi, "Current Research Landscape of Machine Learning Algorithms in Online Identity Fraud Prediction and Detection",2021 IEEE International Conference on Technology Management Operations and Decisions (ICTMOD), pp. 1-6, 2021.

**[11]** L. Beltzung, A. Lindley, O. Dinica, N. Hermann and R. Lindner, "Real-Time Detection of Fake-Shops through Machine Learning",2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 2254-2263

**[12]** F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey", Future Internet, vol. 11, no. 4, p. 89, 2019.

**[13]** S. Carta, G. Fenu, D. Reforgiato Recupero and R. Saia, "Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model", Journal of Information Security and Applications, vol. 46, pp. 13-22, June 2019

**[14]** C. Carpineto and G. Romano, "Learning to detect and measure fake ecommerce websites in search-engine results",Proceedings of the International Conference on Web Intelligence, pp. 403-410, August 2017.

**[15]** A. Abbasi, Z. Zhang, D. Zimbra, H. Chen and J. F. Nunamaker, Detecting Fake Websites: The Contribution of Statistical Learning Theory", MIS Quarterly, vol.34, no.3, pp.435-461, September 2010.