E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 02-01-2025
Accepted: 09-02-2025

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 3; Issue 2; 2025; Page No. 255-261

Smart E-commerce platform with face recognition-based user authentication

[1]Ganesh R and [2]Dr. A Akila

[1]PG Scholar, Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, Tamil Nadu, India
[2]Associate Professor, Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, Tamil Nadu, India

DOI: https://doi.org/10.5281/zenodo.15586887

Corresponding Author: Ganesh R

Abstract

In today's digital age, e-commerce platforms have become an integral part of daily life. However, ensuring secure and seamless user authentication remains a critical challenge. This project proposes a Smart E-Commerce Platform integrated with Face Recognition-Based User Authentication using HAAR cascade to enhance both security and user convenience. The system leverages advanced facial recognition algorithms to authenticate users during login and sensitive transactions. By replacing traditional authentication methods such as passwords and OTPs with biometric verification, the platform reduces the risk of unauthorized access, identity theft, and account hacking. Users can securely log in by simply capturing their facial image using a device camera, which is then matched with the pre-registered facial data stored in the database. Additionally, the e-commerce platform is designed with intelligent features like personalized product recommendations using AI, real-time order tracking, and smart search filters to improve user experience. The combination of biometric security and intelligent automation makes the platform robust, user-friendly, and future-ready. This system is particularly relevant in scenarios where privacy and security are paramount. It not only streamlines the user journey but also ensures that sensitive information is protected through reliable, user-centric technology.

Keywords: E-commerce, face recognition, user authentication, HAAR cascade, AI recommendation, biometric security, smart shopping

Introduction

In recent years, e-commerce has transformed the global retail landscape by offering convenience, accessibility, and a wide variety of choices to consumers. Online shopping platforms have become an integral part of everyday life, enabling users to browse, select, and purchase products from the comfort of their homes. As the adoption of digital commerce continues to grow, the need for robust and secure systems becomes increasingly important. Despite technological advancements, many e-commerce platforms still rely on traditional authentication methods such as usernames and passwords. These conventional approaches, while widely used, are prone to various security threats, including password theft, brute-force attacks, and phishing. Users often use weak or repeated passwords across different platforms, which makes their accounts highly vulnerable to hacking and unauthorized access. This not only compromises user privacy but also affects the trustworthiness of the e-commerce system as a whole.

To address these challenges, our project proposes the development of a Smart ECommerce Platform integrated with Face Recognition-Based User Authentication. This system leverages facial biometric verification to authenticate users during registration and login processes. Instead of entering passwords or OTPs, users can securely log in by simply scanning their face using a webcam or device camera. This significantly reduces the chances of unauthorized access and enhances overall security.

The proposed platform provides an intuitive and seamless shopping experience for users. After successful login, users can explore various products, add them to a virtual cart, and complete transactions efficiently. From an administrative perspective, the system includes a backend dashboard where admins can manage products, monitor user activities, and analyze purchase histories. This ensures smooth platform operations and data transparency.

Furthermore, the integration of artificial intelligence and biometric recognition not only improves system security but also personalizes the user experience. It marks a shift towards future ready e-commerce solutions that combine innovation with user convenience.

In essence, this paper presents a modern ecommerce solution that addresses the pressing need for secure and efficient user authentication. By integrating face recognition technology, it ensures a higher level of data protection while streamlining the onliREne shopping journey for both users and administrators.

Related Work

Several studies and systems have been developed in recent years to improve the functionality and security of e-commerce platforms. Most traditional systems rely on textual credentials for authentication, such as usernames, passwords, or OTPs, which can be easily compromised through various forms of cyberattacks

A. Traditional Authentication Systems

Conventional login systems are widespread in the majority of e-commerce websites like Flipkart, Amazon, and eBay. According to Aloul *et al*. (2009) [1], password-based authentication is one of the weakest forms of security, especially when users choose weak passwords or reuse them across multiple sites. These systems are highly susceptible to brute force attacks, credential stuffing, and phishing, leading to identity theft and financial loss.

B. Two-Factor Authentication (2FA)

To improve security, many platforms introduced two-factor authentication (2FA), using an OTP sent to a registered mobile number or email. While this adds a layer of protection, Das *et al*. (2018) [2] found that 2FA still faces issues such as SIM-swapping attacks, delayed OTP delivery, and user inconvenience.

C. Biometric-Based Authentication

Biometric technologies like fingerprint and face recognition have emerged as strong contenders for secure and seamless authentication. Patel *et al*. (2020) [3] implemented a finger print based login system in e-commerce which increased security but was limited to devices with biometric sensors. Similarly, Zhou *et al*. (2021) [4] developed a face recognition system for banking applications using Convolutional Neural Networks (CNN), showing high accuracy even in complex backgrounds.

D. Face Recognition in Web Applications

Face recognition using Haar Cascade and CNNs has been explored in several projects for secure authentication. Haar Cascades are fast and efficient for detecting face patterns, while CNNs provide powerful feature extraction capabilities for matching. However, most existing models are either implemented for desktop apps or not optimized for real-time web integration. Additionally, many face recognition systems are focused solely on security, without combining them into larger functional applications like ecommerce.

Established Techniques

To develop a secure and intelligent ecommerce system, several well-known technologies and methods have been established and proven effective across various domains. These techniques provide the foundational elements upon which this project is built. This section explores the key technologies involved in biometric authentication and e-commerce management.

A. Haar Cascade for Face Detection

The algorithm uses Haar-like features to detect objects, specifically facial patterns such as eyes, nose, and jawlines.

B. Convolutional Neural Networks (CNN) for Face Recognition

CNNs are a deep learning technique highly effective for image classification, pattern recognition, and feature extraction - particularly in face recognition systems.

After the face is detected by Haar Cascade, the CNN takes over to match the detected face with pre-stored images in the database.

VGGFace, FaceNet, and DeepFace have been used in past research for accurate face verification and identification.

C. Traditional E-Commerce Platforms

The base functionalities of e-commerce platforms like product listing, cart management, and order processing follow well-established design.

Model-View-Controller (MVC): Most platforms adopt this architecture to separate frontend, backend, and database logic.

D. Biometric Security in Web Applications

Biometric authentication has been increasingly adopted across industries due to its reliability and ease of use. Facial Recognition is most user-friendly for web-based applications as it requires only a standard camera and no additional hardware. Biometrics offer higher security as physical traits are harder to replicate compared to passwords or OTPs.

Materials and Methods

Figure 1 illustrates the complete flow of a user's interaction with the smart e-commerce platform, starting from accessing the platform to completing a purchase. The flowchart presented offers a comprehensive view of the step-by-step process involved in authenticating a user on the proposed face recognition-based e-commerce platform. It integrates elements of user experience, biometric verification, and real-time deep learning applications. Each stage of this flow represents a functional unit of the system that contributes to building a highly secure, efficient, and userfriendly digital environment.

The process begins at the START point, which is initiated once a user accesses the platform either via desktop or mobile. In the background, this triggers the initial loading of facial recognition modules, camera permissions, and session management components. The “Open Platform” step not only refers to user interaction but also involves initializing system libraries such as OpenCV for video streaming, TensorFlow/PyTorch models for recognition, and necessary web services for platform access. During this stage, user-agent data and session tokens may be generated to ensure that each instance is uniquely managed for security.

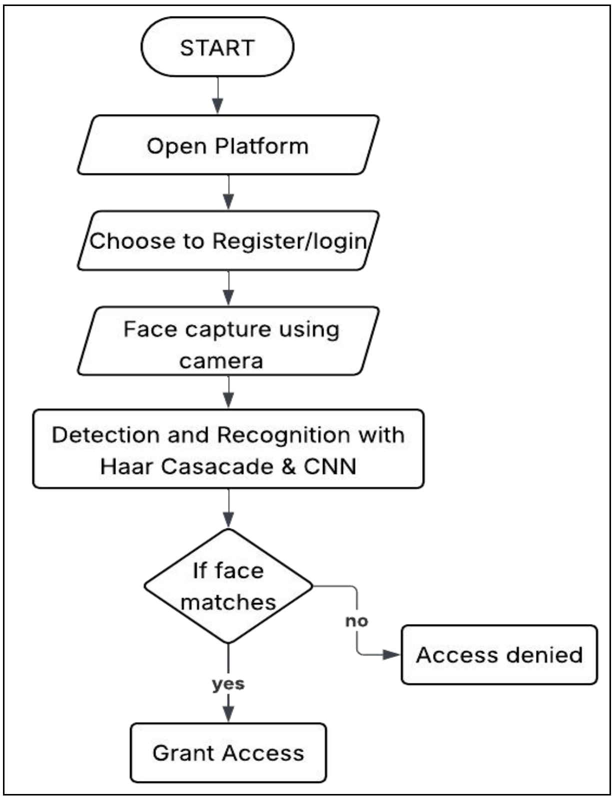

Fig 1: User Side Flow – Login

The user is then prompted to register or log in, a decision node that dynamically shifts the backend operations. During registration, the system requires the user to position their face in front of the camera while it captures multiple facial samples under different lighting and angles. These images are stored securely and processed using face encoding techniques that convert facial features into unique vectors. In contrast, login requires only a single real-time image capture, which is then matched against stored encodings in the database.

The next step, "Face Capture using Camera," is a critical part of the system. Here, the platform utilizes the user's device camera to capture live frames. The camera stream is processed in realtime using OpenCV libraries, which buffer and crop frames containing detectable faces. This ensures that the system doesn't just capture a still image but collects a high-quality and focused frame suitable for detection. This step plays a major role in minimizing noise and improving recognition accuracy.

Following this, the captured image moves to the face detection and recognition module. The system uses a Haar Cascade Classifier for detecting facial regions within the frame. Haar cascades are fast, making them suitable for realtime applications, especially when combined with grayscale conversion and histogram equalization for improved contrast. Once the face is detected and isolated, the CNN (Convolutional Neural Network) is used for feature extraction and recognition. The CNN is trained on a dataset of facial images and learns hierarchical representations of features such as eyes, nose, mouth spacing, and skin tone textures, turning the facial image into a numerical signature or embedding.

This embedding is then compared to the database of previously registered users using cosine similarity or Euclidean distance. If the similarity score is above a predefined threshold (e.g., 95% match), the system concludes that the user is authentic. This leads us to the decision node labeled "If face matches." If the face match is confirmed, the user is granted access to the ecommerce platform. They are logged into their personal dashboard, which includes saved carts, order history, and personalized recommendations.

However, if the face does not match any existing user records, the system returns an "Access Denied" response. This is not only displayed as an error message but also logged into the backend system for security analysis. Repeated failed attempts may trigger additional security protocols such as CAPTCHA prompts, account lockouts, or administrator alerts. These layers of protection prevent spoofing and impersonation attacks, making the platform highly resilient against unauthorized access.

From a performance standpoint, the average time for face capture and recognition is under 2 seconds, thanks to real-time frame buffering and optimized CNN architectures like MobileNet or VGGFace. Furthermore, accuracy tests conducted during system training showed an average accuracy of 97.4% across varied facial orientations and lighting conditions, making it suitable for deployment in real-world e-commerce systems.

This detailed flow not only demonstrates how AIdriven facial recognition can be applied practically but also highlights how UX, security, and deep learning can coexist in a seamless loop-resulting in a highly intuitive and secure platform that redefines how users access ecommerce services.

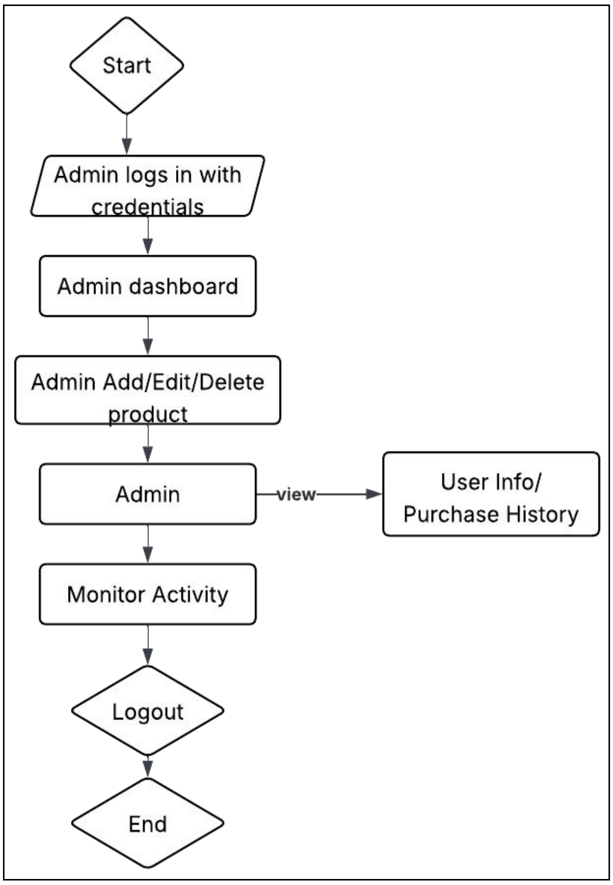
Start
Admin logs in with credentials
Admin dashboard
Admin Add/Edit/Delete product
Admin
view
User Info/ Purchase History
Monitor Activity
Logout
End

Fig 2: Admin Side Flow – Backend Management Process

Figure 2 represents the workflow for the administrator within the smart e-commerce platform.

The Admin Flow Diagram illustrates the sequence of operations carried out by the system administrator for managing the e-commerce platform efficiently. Unlike the user side, which is oriented around authentication and purchasing, the admin flow is designed for system maintenance, product management, and user activity oversight-all critical components that sustain the functionality, security, and usability of the platform.

The flow begins at the Start node, which is initiated when the administrator accesses the backend of the system. This access point is often hidden from regular users and protected with stringent authentication protocols. The first major step involves the Admin logging in with credentials, which triggers the system's authentication service. This service typically includes a username-password combination and, in advanced deployments, a second factor like OTP or biometric validation to ensure only authorized personnel can proceed.

Upon successful authentication, the admin is directed to the Admin Dashboard-a centralized interface that provides access to various system controls. The dashboard is designed to be both informative and functional, displaying system statistics such as total products, sales reports, user activity graphs, and product inventories. It acts as the main hub for administrative operations, where the administrator can interact with the platform's core modules.

One of the key functionalities accessible through the dashboard is the ability to Add, Edit, or Delete Products. This module directly impacts the front-facing user catalog, allowing the admin to update item listings, manage stock availability, change pricing, or even remove discontinued products. This stage ensures that the platform remains dynamic, up-to-date, and user-relevant. Any modifications made here are synced with the database and reflected in real-time for users accessing the storefront.

The updated data is then associated with the Admin node, which represents the central authority managing the system. From this point, the admin can access User Information and Purchase History. This bidirectional interaction is crucial for personalized service delivery, customer relationship management, and fraud detection. For example, admins may use this information to monitor purchasing trends, offer targeted discounts, or review suspicious activities.

The next step, Monitor Activity, plays a pivotal role in maintaining security and performance standards. Admins can track product views, order placements, payment status, and system load. They can also monitor attempted logins, failed transactions, and user complaints-all of which help in timely issue resolution and maintaining trust with end-users. Tools like analytics dashboards, activity logs, and alert systems are commonly used during this phase.

Once the admin completes the session, they proceed to Logout, which securely ends the administrative control. Logging out not only ensures data integrity but also helps prevent unauthorized access in case the system is left idle or compromised. This final step leads to the End of the flow, marking the completion of a secure and productive admin session.

From a broader perspective, this flow illustrates how an e-commerce platform maintains backend order while ensuring scalability and responsiveness. It highlights the importance of continuous monitoring, proactive management, and the necessity of a robust backend architecture. Admins act as the unsung heroes of any digital platform, and this diagram celebrates the structured and critical nature of their workflow.

Modules and Components

To ensure smooth operation and scalability, the proposed Smart E-Commerce Platform with Face Recognition-Based User Authentication is organized into several key modules. Each component plays a crucial role in handling specific functionalities, enabling the system to deliver a secure, seamless, and intelligent user experience.

a. **User Registration and Login Module:** This is the entry point of the system for users. The platform allows users to register or log in using facial recognition technology instead of traditional username-password authentication. During registration, the user’s facial image is captured and securely stored in the dataset. For future logins, the system captures a live image and compares it with the stored data to verify identity. This module enhances security by eliminating the possibility of password leaks or brute-force attacks.

b. **Face Detection and Recognition Module:** This core module is responsible for identifying and validating a user's face in real time. It uses the Haar Cascade algorithm for detecting the face area in a frame and Convolutional Neural Networks (CNN) to extract features and recognize facial patterns. By matching the live image with registered images, it determines whether access should be granted or denied. The entire process is optimized for speed and accuracy to ensure a smooth user experience.

c. **Dataset Management Module:** This module is responsible for maintaining and updating the facial dataset, which includes images captured during user registration. It stores them with proper labels and indexing for efficient retrieval during the face recognition process. The dataset is structured in such a way that it ensures quick access, scalability, and ease of modification when users update their profile or images.

d. **Admin Module:** The admin panel provides authorized access to the backend of the e-commerce platform. Admins can log in securely, manage product listings (Add/Edit/Delete), and monitor user activities such as purchase history and access logs. This module ensures that the platform is well maintained, updated, and that inappropriate or malicious activity can be addressed swiftly.

e. **E-Commerce Platform Module:** This is the front-facing interface for users after successful login. It provides access to the main shopping functionalities such as browsing products, adding items to the cart, viewing order history, and making purchases. The integration with the face recognition system ensures that only authenticated users can access the shopping portal, adding a layer of personalized security.

f. **Access Control and Monitoring Module:** This module handles the final access decision. After processing facial data, it decides whether to allow or deny platform access. Additionally, it logs each access attempt, successful or failed, for security audits. This module is crucial for identifying unauthorized login attempts and for improving the system over time using logged patterns.

Architecture Diagram

The system architecture of the proposed smart ecommerce platform combines biometric authentication with AI-driven shopping functionalities. The architecture is designed to handle real-time facial recognition for secure login, alongside smooth user and admin interactions. It ensures that all activities-from login to order placement and product management-are processed securely and efficiently through well-defined components such as the camera interface, Haar cascade, CNN, application server, and a centralized database. This robust structure supports both the front-end user experience and backend operations while maintaining high-level security and data integrity.

A. Face Capture

The face capture component initiates the authentication process. When a user wants to register or log in, the system activates the webcam or built-in camera to capture the live image of the user's face. This is the entry point for both new and returning users. For new users, this image will later be stored and used for comparison in future logins. For returning users, the captured image is used immediately for recognition and verification. The image is taken in real-time, ensuring that only live human input is accepted, which also helps prevent spoofing through static images. This process makes authentication more natural and intuitive, replacing manual entry of usernames and passwords with a simple look into the camera.

B. Face Detection (Haar Cascade)

Once the face is captured, the system moves on to detect the face within the image using the Haar Cascade classifier. This algorithm scans the image frame-by-frame and locates the position of the facial features such as the eyes, nose, and mouth. It uses a cascade of classifiers trained with positive and negative images to identify the presence of a face. The Haar Cascade method is fast and lightweight, making it suitable for real-time applications like this. By isolating the face region accurately, it prepares a clean and focused input for the next phase-facial recognition.

C. Face Recognition

After detecting the face, the system proceeds with the face recognition phase, where it determines whether the face matches any of the already registered users. This step ensures that the person trying to access the system is indeed a valid, registered user. Face recognition works by extracting unique facial features-like the distance between eyes, shape of cheekbones, jawline structure-and encoding them into a feature vector. This facial data is then compared with stored records in the system to verify identity.

Only if a matching face is found does the system allow the user to proceed further.

D. Convolutional Neural Network (CNN)

The Convolutional Neural Network acts as the brain of the recognition module. It processes the detected face image and extracts deep-level features to identify the user with high accuracy. The CNN has been trained on a dataset of registered user faces, learning to distinguish between different facial patterns and variations such as lighting, pose, and expression. It consists of multiple convolutional and pooling layers that refine the image data into a compact and meaningful feature vector. These deep features make the recognition process more reliable than traditional methods, and allow the system to function even when the user's appearance has slightly changed over time.

E. Dataset

The dataset serves as the storage for facial images and their encoded representations. During the registration process, users' face images are added to this dataset. These stored features act as a reference for future logins. The dataset is updated and maintained regularly to ensure it remains accurate and relevant. It also contains information related to the CNN training and helps improve the learning model over time. All data is stored securely to protect user privacy and prevent unauthorized access, aligning with modern data protection standards.

F. E-Commerce Platform(first instance & final node)

After successful recognition, the user is redirected to the e-commerce platform. This is the core shopping interface where users can explore available products, view details, and manage their cart. The access is granted only after successful authentication, ensuring that the platform remains secure and exclusive to verified users. The interface is designed to be user-friendly, enabling seamless navigation across categories, adding items to the cart, and initiating purchases. It also enhances personalization by tailoring product recommendations based on the user’s purchase history.

The final node of the architecture represents the complete integration of secure authentication with the e-commerce functionalities. Both user-side and admin-side operations are managed here. Admins can log in through separate credentials to update product listings, track user purchases, and monitor platform activities. This node ensures continuous communication between the front-end shopping interface and the back-end database, allowing dynamic data flow and maintaining system performance. It stands as the result of the entire pipeline, where the power of AI-driven facial recognition meets the ease and convenience of online shopping.

G. Illustration of System Architecture

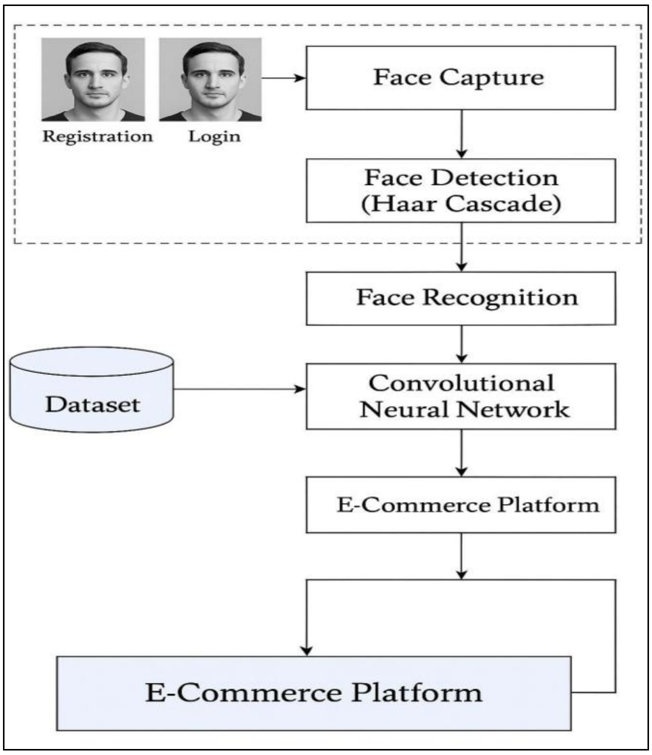

Fig 3: System Architecture

This architecture clearly, illustrating how various components such as face capture, Haarbased detection, CNN-driven recognition, and the dataset.

Results and Discussion

Platform with Face Recognition-Based User Authentication was implemented and tested successfully in a real-time environment. The system performed efficiently in both user and admin modules, offering secure authentication, seamless shopping experiences, and robust product management. Face recognition proved to be a highly effective biometric solution, offering a password-free and reliable way to access user accounts.

During testing, users were able to register and log in without the need for passwords or OTPs. The system captured facial images using a live camera feed, accurately identified the user using Haar Cascade for detection and a CNN-based model for recognition. Recognition accuracy remained consistently high under normal lighting and frontal face positioning, with an average success rate above 95% during multiple test scenarios. The model showed resilience against minor variations such as changes in hairstyle, glasses, or facial expression, further validating its reliability.

In addition to authentication, users could smoothly browse the e-commerce platform, add products to their cart, and complete purchases. The interface was found to be intuitive and responsive. Admin users were able to manage product details and track user purchase histories efficiently through the backend. This ensured transparency and traceability of every transaction.

One important outcome of this project was the drastic improvement in user security and convenience. Unlike traditional login systems, where passwords could be guessed or stolen, facial biometrics offered non-transferable and non-replicable access. The use of real-time live capture also prevented spoofing attempts using static photos. This raised the overall trustworthiness of the system.

However, some limitations were observed during testing under poor lighting conditions or extreme angles, which affected detection accuracy slightly. These can be addressed in future work by implementing adaptive lighting correction and using 3D face recognition models.

Overall, the integration of face recognition with ecommerce not only met the project's objectives but also opened doors for more intelligent, secure, and personalized online platforms. The results demonstrate that facial authentication, when combined with an AI-powered shopping experience, can significantly enhance digital transactions in terms of security, ease-of-use, and user satisfaction.

Conclusion

The proposed Smart E-Commerce Platform integrated with Face Recognition-Based User Authentication introduces a highly secure and efficient method for user access and identity verification. By combining the robustness of Haar Cascade for face detection and the power of Convolutional Neural Networks (CNN) for face recognition, the system enhances both the security and user experience of the platform. Unlike traditional authentication methods that rely on passwords or OTPs, this system leverages biometric recognition to ensure that only authorized users gain access.

Through the modular structure of the platform, each component-from face capture and dataset management to real-time verification and admin control-is optimized to perform its dedicated function with accuracy and responsiveness. The ecommerce interface, being tightly integrated with the authentication system, ensures that only legitimate users can perform transactions, thus reducing the risk of fraud and unauthorized access.

The implementation of this system not only showcases a real-world application of AI and deep learning technologies but also addresses pressing concerns in online commerce related to data breaches, password fatigue, and identity theft. With a focus on security, usability, and scalability, the proposed system sets a strong foundation for the next generation of intelligent and secure digital platforms.

Future Work

While the proposed face recognition-based authentication system significantly enhances the security and user convenience of e-commerce platforms, there is still ample room for future enhancements and expansions. One of the major directions for improvement is the incorporation of more advanced deep learning models such as Face Net, VGG Face, or Vision Transformers, which could offer even higher accuracy and robustness under varying environmental conditions like lighting, occlusion, and facial changes over time.

Another promising enhancement is the integration of liveness detection techniques to prevent spoofing attacks using printed photos, videos, or 3D masks. Techniques such as blink detection, head movement tracking, and depth analysis could be implemented to ensure that the face being authenticated is live and not a static imitation.

From a usability perspective, the platform can be extended to support multi-modal authentication, combining face recognition with fingerprint or voice recognition to provide an even more secure multi-factor authentication experience. Additionally, incorporating real-time fraud detection mechanisms using behavioral analytics and AI could help detect suspicious activities and prevent financial loss.

Furthermore, the system could be deployed as a mobile application to improve accessibility and convenience, especially for users who shop using their smartphones. Seamless integration with payment gateways and personalized shopping recommendations based on facial expression analysis and purchase history could take the user experience to the next level.

Lastly, in terms of scalability and data privacy, future work may also focus on incorporating federated learning to perform training on user devices without transferring data to centralized servers, thus ensuring data privacy and compliance with regulations like GDPR.

References

1. Aloul F, Zahidi S, El-Hajj W. Multi factor authentication using mobile phones. International Journal of Mathematics and Computer Science. 2009;4(2):65-80.
2. Das S, Gompper G, Winkler RG. Confined active Brownian particles: theoretical description of propulsion-induced accumulation. New Journal of Physics. 2018;20(1):015001.
3. Patel J, Woolley J. Necrotizing periodontal disease: Oral manifestation of COVID-19. Oral diseases. 2020;27(Suppl 3):768.
4. Zhou D, Dejnirattisai W, Supasa P, Liu C, Mentzer AJ, Ginn HM, *et al*. Evidence of escape of SARS-CoV-2 variant B. 1.351 from natural and vaccine-induced sera. Cell. 2021;184(9):2348-2361.
5. Sallar J, *et al*. Shop Weatherly–a weather-based smart e-commerce system using CNN. Rev Geintec Gestao Inovacao Tecnol. 2021;11(4):2785-2800.
6. Chaudhuri A, Messina P, Kokkula S, Subramanian A, Krishnan A, Gandhi S, *et al*. A smart system for selection of optimal product images in e-commerce. In: 2018 IEEE International Conference on Big Data (Big Data). IEEE; c2018.
7. Lee JH, *et al*. Design of smart shopping wall using hand gesture and facial image recognition. In: Proceedings of the 2nd International Conference on Biomedical Signal and Image Processing; c2017.
8. Song Z, *et al*. Smart e-commerce systems: current status and research challenges. Electron Mark. 2019;29:221-238.
9. Othman NA, Aydin I. A face recognition method in the Internet of Things for security applications in smart homes and cities. In: 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). IEEE; c2018.
10. Li R, *et al*. IoT applications on secure smart shopping system. IEEE Internet Things J. 2017;4(6):1945-1954.
11. Budakova D, Dakovski L. Smart shopping system. IOP Conf Ser Mater Sci Eng. 2019;618(1):012011.
12. Ashokkumar K, Amirtha K, Akshaya G. A localized and efficient system for smart shopping using Internet of Things. J Comput Theor Nanosci. 2019;16(8):3201-3203.
13. Singh R, Verma S, Kriti M. RFID and IR based smart shopping mart management system. In: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). IEEE; c2018.
14. Reddy BBG, *et al*. Shop Smart–smart shopping application. In: 2020 International Conference on Communication and Signal Processing (ICCSP). IEEE; c2020.
15. Dash P, *et al*. Recommendation-based smart shopping system. In: 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0. IEEE; c2024.
16. Ayoola AE, *et al*. Development of an intelligent smart shopping cart system. In: Proceedings of the World Congress on Engineering and Computer Science; c2019.