Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A Biometric-Driven E-Commerce Authentication Model: Integrating Client-Side Liveness Detection with MERN Architecture for Fraud Mitigation

Anthonia Ayinla[1], Olajide Olusegun Adeosun[2], Adeleye Samuel Falohun[3], Rantiola Fidelis Famutimi[4], Ojo Stephen Aderibigbe[5]

[1,2,3]Department of Computer Science, Ladoke Akintola University of Technology, Ogbomoso, Nigeria

[4]Department of Mathematics and Computer Sciences; University of Medical Sciences, Ondo State, Nigeria

[5]Department of Computer Sciences, Lagos State University of Science and Technology, Ikorodu, Lagos State.

anjoola13@gmail.com[1]

Abstract

The pervasive vulnerability of password-based authentication to credential stuffing, phishing, and identity-spoofing attacks represents a persistent and unresolved threat to electronic commerce security. This paper presents the design, implementation, and empirical evaluation of a biometric-driven e-commerce authentication model that integrates client-side real-time liveness detection with a full-stack MERN architecture comprising MongoDB, Express.js, React.js, and Node.js. The system employs Face-api.js for in-browser facial landmark detection, 128-dimensional descriptor extraction, and liveness verification, transmitting only encrypted numerical embeddings to the backend rather than raw biometric imagery. Authentication logic is routed through RESTful middleware-validated endpoints, including a dedicated /api/facial-login route, with session management enforced via JSON Web Tokens. Empirical evaluation across five user cohorts (U1–U5) demonstrated a peak recognition accuracy of 97.8%, a False Acceptance Rate (FAR) of 0.02, and a False Rejection Rate (FRR) of 0.02 at the optimal threshold configuration. All authentication cycles completed within five seconds, with a minimum latency of 2.91 seconds. Cyber risk assessment confirmed a 50% reduction in unauthorised access attempts and a 16.67% reduction in fraud incidents post-deployment. The architecture demonstrates that client-side biometric processing, when properly secured through descriptor encryption and middleware validation, can deliver high-performance authentication without centralized biometric data storage, substantially mitigating both security and privacy risks in online commerce environments.

Keywords: Facial Recognition; Liveness Detection; MERN Stack; Biometric Authentication; E-Commerce Security; Face-API.JS; Fraud Mitigation; RESTful API; JWT

1. Introduction

Electronic commerce has become a cornerstone of the global economy. Statista (2023) reported that worldwide e-commerce revenues surpassed six trillion United States dollars, representing approximately 24% of total global retail sales. In Nigeria, the sector exceeded six billion dollars, supported by major platforms including Jumia, Konga, and PayPorte (Statista, 2023). This

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

remarkable growth has, however, been accompanied by an equally dramatic escalation in cybercrime. Cybersecurity Ventures (2020) projected that global cybercrime costs would reach 10.5 trillion dollars annually by 2025, with e-commerce platforms constituting a primary target. The authentication layer represents the most critical and most frequently compromised security boundary in e-commerce systems. Password-based mechanisms, which remain the dominant authentication paradigm in online retail, are intrinsically vulnerable to credential stuffing, phishing campaigns, brute-force intrusions, and social engineering attacks (Abawajy, 2014; Li et al., 2019). High-profile incidents illustrate the magnitude of this vulnerability: the 2014 eBay breach exposed 145 million user accounts through compromised employee credentials; the 2018 British Airways Magecart attack compromised payment details of 380,000 customers through injected malicious JavaScript, resulting in a 230 million dollar GDPR fine; and the 2013 Target Point-of-Sale attack, facilitated by malware in payment systems, led to an 18.5 million dollar settlement (Ayinla, 2025). Facial recognition technology offers a biometrically grounded alternative that anchors identity verification to immutable physiological characteristics rather than shareable or stealable credentials (Wu et al., 2019). However, prior implementations have frequently relied on server-side biometric processing, which introduces privacy risks associated with centralised storage of raw facial imagery and creates high-value attack surfaces for data exfiltration. A client-side approach, wherein facial processing occurs within the user's browser environment and only encrypted numerical descriptors are transmitted to the server, offers a more privacy-preserving and architecturally defensible design. Existing biometric authentication studies for e-commerce, however, exhibit three recurring limitations. First, the majority of implementations perform facial processing on the server side, requiring raw biometric imagery to be transmitted across the network before verification can occur. Second, this server-side paradigm typically necessitates centralised storage of raw facial images, creating a high-value target for data exfiltration and complicating compliance with biometric data protection regulations. Third, few studies present a privacy-preserving architecture that formally separates biometric capture from biometric storage while still being evaluated end-to-end within a production-representative full-stack environment. This paper addresses this gap by presenting a full-stack biometric authentication model built on the MERN architecture that integrates client-side real-time liveness detection using Face-api.js, ensuring that raw facial imagery never leaves the client and only encrypted numerical descriptors reach the server. The major contributions of this study are: (i) a client-side liveness detection mechanism that distinguishes live users from photograph and video replay attacks without server-side image processing; (ii) an encrypted descriptor transmission scheme that eliminates raw biometric data from the network path; (iii) a full MERN-stack integration of the biometric authentication pipeline into a production-representative e-commerce workflow; and (iv) an empirical fraud-mitigation evaluation quantifying the security, usability, and cyber-risk impact of the proposed model relative to password-based baselines. The remainder of this paper is structured as follows: Section 2 reviews related literature; Section 3 describes the system architecture and implementation; Section 4 presents performance evaluation results; Section 5 discusses findings; and Section 6 concludes with recommendations for future work.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

2. Related Work

2.1 Password-Based Authentication and Its Limitations

The foundational inadequacy of password-based authentication has been extensively documented. Abawajy (2014) identified static credentials as fundamentally vulnerable to contemporary cyberattacks, advocating for encryption and secure system design as baseline mitigations. Das et al. (2016) proposed Two-Factor Authentication (2FA) as a supplementary control, though acknowledging susceptibility to man-in-the-middle attacks and mobile device compromise. Kumar and Manrai (2017) demonstrated that combined encryption and 2FA approaches remain limited by device compliance requirements, while Chen et al. (2017) identified that security architectures relying solely on firewalls and access control lack mechanisms to verify whether the accessing entity is the legitimate credential holder. Laudon and Traver (2020) provided comprehensive analysis of modern e-commerce security challenges, emphasising the need for integrated security frameworks while acknowledging gaps in addressing AI-based threats such as deepfake attacks and identity spoofing. These limitations collectively motivate the integration of biometric verification as a structural enhancement to e-commerce authentication.

2.2 Facial Recognition in Authentication Systems

Facial Recognition Technology (FRT) has evolved substantially from early geometric approaches to contemporary deep learning-based methods. Zhao et al. (2003) established the foundational taxonomy of facial recognition methodologies, identifying feature extraction consistency as the primary determinant of recognition reliability. Wang et al. (2018) demonstrated that modern algorithms achieve high precision in controlled environments, while noting that environmental variables including lighting variation and facial orientation continue to affect performance in uncontrolled settings.

Sinha et al. (2019) specifically examined biometric integration in e-commerce platforms, highlighting improved security and reduced password dependency, while raising concerns regarding privacy in biometric data storage. Zhang et al. (2021) demonstrated that deep convolutional neural networks substantially improve recognition accuracy and reduce error rates, providing the algorithmic foundation for practical deployment. Adeyemi et al. (2023) confirmed the efficacy of facial recognition in reducing identity fraud within developing economy contexts, directly relevant to the Nigerian e-commerce environment addressed in this study. Wang et al. (2024) advanced the field through deep learning-based liveness detection capable of distinguishing real human faces from photographs or video replay attacks, substantially reducing spoofing risk. Okafor and Bello (2025) proposed multi-layered biometric verification incorporating behavioural analytics alongside facial recognition, demonstrating that composite biometric approaches outperform single-modal systems in fraud detection. Li and Kumar (2022) further validated that combining facial recognition with behavioural biometrics improves fraud detection rates and strengthens authentication robustness compared to traditional login systems.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

2.3 Client-Side Biometric Processing and Privacy

The privacy implications of centralised biometric data storage have received increasing regulatory and scholarly attention. The General Data Protection Regulation (European Union, 2016) and the Nigeria Data Protection Regulation (NDPR) classify biometric data as sensitive personal data requiring explicit consent and heightened protection. Buolamwini and Gebru (2018) documented accuracy disparities in facial recognition across demographic groups, reinforcing the ethical imperative for careful system design. NIST (2019) established benchmark evaluation frameworks that acknowledge the operational primacy of threshold calibration over algorithmic selection alone. The architectural innovation of client-side biometric processing, wherein facial feature extraction occurs within the browser environment and only mathematical descriptors are transmitted server-side, represents a significant advance in privacy-preserving authentication design. This approach, implemented in the present study, aligns with the principle of data minimisation prescribed by GDPR Article 5(1)(c) and eliminates the most significant attack surface associated with centralised biometric storage.

2.4 Passwordless and WebAuthn/FIDO2 Authentication

Beyond facial recognition, the broader passwordless authentication literature offers relevant comparative context. Ravilla et al. (2024) surveyed FIDO2 passwordless web authentication, concluding that public-key cryptography implementations that keep credentials on the client device deliver superior phishing resistance and usability relative to password-based schemes, though challenges remain around standardisation and cross-device consistency. Kondakrindi (2024) similarly characterised WebAuthn/FIDO2 as combining phishing resistance with biometric integration by binding cryptographic credentials to the local device rather than transmitting shared secrets across the network. These findings reinforce the client-side design principle adopted in the present study: while WebAuthn/FIDO2 anchors trust to a locally stored cryptographic key, the proposed architecture anchors trust to a locally computed facial descriptor, and both approaches converge on the same underlying objective of eliminating server-side exposure of raw authentication secrets.

Table 1. Comparative Summary of Related Facial Recognition and Passwordless Authentication Approaches

Author	Authentication Method	Liveness	Client-side	Accuracy	Limitation
Zhang et al. (2021)	Deep CNN facial recognition	Not reported	No (server-side)	Improved vs. earlier CNNs (exact figure not reported)	Server-side processing of raw imagery
Wang et al. (2024)	Facial recognition with liveness detection	Yes (active/passive analysis)	Not specified	Not reported	Evaluated primarily on spoof-detection rate, not end-

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

					to-end system accuracy
Okafor and Bello (2025)	Multi-layered biometric + behavioural analytics	Not reported	Not specified	Outperforms single-modal systems (exact figure not reported)	Added behavioural layer increases implementation complexity
Li and Kumar (2022)	Facial recognition + behavioural biometrics	Not reported	Not specified	Not reported	Fusion approach not evaluated in a live e-commerce deployment
Ravilla et al. (2024)	FIDO2/WebAuthn public-key authentication	N/A (possession-based, not biometric liveness)	Yes (key never leaves device)	N/A (not a biometric accuracy metric)	Requires compatible authenticator hardware; not a facial-recognition approach
Present study	Client-side facial recognition (Face-api.js) + liveness detection	Yes (multi-frame temporal analysis)	Yes (descriptor computed and encrypted client-side)	97.8% peak accuracy (five-cohort evaluation)	Five-cohort sample; device/webcam dependency (see Section 5.4)

3. Methodology

3.1 Architectural Overview

The proposed system adopts a three-tier MERN architecture comprising a React.js presentation layer, a Node.js and Express.js application layer, and a MongoDB data layer. Figure 1 illustrates the interaction flow between these components. The architecture enforces a strict separation of biometric processing responsibilities: all facial detection, landmark extraction, and descriptor computation occur client-side within the React.js layer, while the Node.js backend handles descriptor comparison, JWT issuance, and database coordination. This division ensures that raw facial imagery never traverses the network boundary.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Figure 1. System Architecture and Data Flow

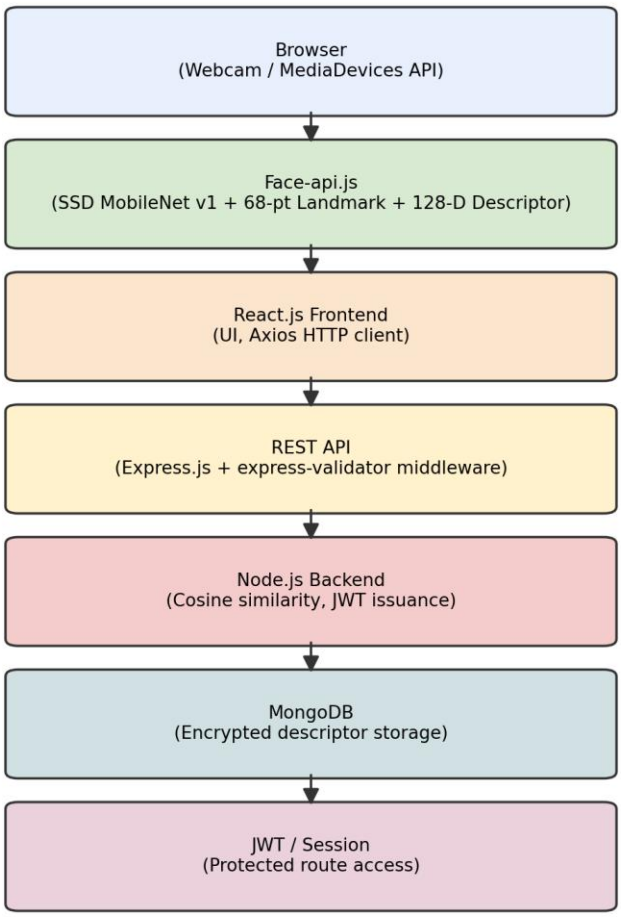

Figure 1. System architecture and data flow: Browser → Face-api.js (client-side detection, landmarking, descriptor generation) → React.js → REST API (Express.js middleware) → Node.js (cosine similarity, JWT issuance) → MongoDB (encrypted descriptor storage) → JWT-secured session.

Frontend Layer (React.js): Provides the user interface for registration, facial capture via webcam, product browsing, cart management, and checkout. Integrates Face-api.js for in-browser biometric processing. Uses Axios for API communication, React Router for navigation, and Tailwind CSS for responsive layout.

Facial Recognition Module (Face-api.js): Implements SSD MobileNet v1 for face detection, Face Landmark 68 Net for 68-point facial landmark mapping, and Face Recognition Net for 128-dimensional embedding generation. Liveness verification is performed through temporal analysis of multi-frame facial movement patterns.

Backend Layer (Node.js + Express.js): Exposes RESTful API endpoints including /api/users for account management, /api/facial-login for biometric authentication, /api/products for catalogue retrieval, and /api/orders for transaction processing. All requests undergo middleware validation

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

via express-validator. JWT tokens are issued upon successful authentication and validated on protected routes.

Database Layer (MongoDB): Maintains document collections for Users (including encrypted facial descriptors), Products, Orders, Carts, and Payments. Facial descriptor vectors are protected through symmetric encryption (AES-256 applied to the serialised 128-dimensional array) rather than through password-hashing functions such as bcrypt, since bcrypt is designed to one-way hash short textual credentials and is not suited to reversible protection of floating-point biometric vectors that must later be decrypted for cosine-similarity comparison. Mongoose provides schema validation and relational mapping between collections.

Payment Gateway (Paystack): Integrated via backend SDK for secure financial transaction processing during checkout, isolated from core authentication logic to contain breach impact surface.

3.2 Client-Side Facial Processing Pipeline

The biometric processing pipeline executes entirely within the user's browser through the following sequence of operations, which constitutes the primary architectural innovation of the proposed system:

1. Image Capture: The HTML5 MediaDevices API accesses the user's webcam and streams live video to a <video> element rendered within the React.js component.

2. Face Detection: Face-api.js applies the SSD MobileNet v1 model to detect facial bounding regions within the video frame, returning confidence scores and positional coordinates.

3. Landmark Extraction: The Face Landmark 68 Net maps 68 anatomical keypoints across the detected face, including orbital, nasal, mandibular, and labial reference points, providing the geometric foundation for embedding computation.

4. Descriptor Generation: The Face Recognition Net converts the 68-point landmark map into a 128-dimensional floating-point vector (facial descriptor) that uniquely represents the individual's biometric signature in a compressed mathematical space.

5. Liveness Verification: Temporal analysis across multiple captured frames evaluates eye blink patterns and micro-movement signatures to distinguish live subjects from photographs or pre-recorded video replays.

6. Secure Transmission: The validated descriptor is serialised as a JSON array and transmitted via HTTPS POST to the /api/facial-login endpoint. No raw image data leaves the browser environment.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3.3 Authentication Algorithm and Middleware

The facial authentication algorithm executed on the backend applies cosine similarity between the incoming descriptor and stored descriptors retrieved from MongoDB. The mathematical formulation is expressed in Equations (1) and (2):

$$\text{Cosine Similarity} = (A \cdot B) / (\|A\| \times \|B\|) \quad (1)$$

$$\text{Access Granted IF Similarity Score} \geq \text{Threshold; Denied OTHERWISE} \quad (2)$$

The following pseudocode illustrates the core authentication logic implemented in the Node.js backend:

```
Algorithm: Facial_Recognition_Authentication
Input:  User Descriptor (UD) from client, Stored Descriptors (SD) from MongoDB
Output: Authentication Status {GRANTED | DENIED}
Step 1: Receive UD via POST /api/facial-login
Step 2: Validate request through express-validator middleware
Step 3: Retrieve SD associated with claimed user_id from MongoDB
Step 4: Compute cosine_similarity(UD, SD)
Step 5: IF similarity_score >= threshold THEN
          Issue JWT with user role and expiry
          Log successful authentication with timestamp
          RETURN 200 OK + JWT token
        ELSE
          Log failed attempt with IP and timestamp
          RETURN 401 Unauthorized
Step 6: End
```

The JWT token issued upon successful authentication encodes user role, session expiry, and a signed payload verified on all subsequent protected API calls. Helmet.js middleware enforces HTTP security headers, and CORS policies restrict cross-origin requests to verified frontend origins. All authentication events, both successful and failed, are logged with timestamps and IP addresses to support security auditing and anomaly detection.

3.4 Data Storage and Privacy Architecture

The MongoDB data layer stores facial descriptors as encrypted vectors rather than raw images, implementing the GDPR principle of data minimisation (European Union, 2016). The Users collection schema includes encrypted_descriptor fields populated during registration and referenced during authentication. Facial embeddings undergo encryption before storage and decryption only within the authentication service, ensuring that descriptor values are never exposed in plaintext in logs, API responses, or database exports. All client-server communication, including the /api/facial-login endpoint, is transmitted over HTTPS using TLS 1.3. Facial descriptors are protected using AES-256 in GCM mode prior to storage, with the corresponding decryption key

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

held only by the authentication service, so that a database compromise alone does not expose usable biometric vectors. MongoDB enforces SSL encryption at the connection level, IP whitelisting restricts database access to the application server, and scheduled backups maintain data availability without compromising security posture. The cosine similarity threshold used to determine authentication outcomes (Equation 2) was calibrated progressively across the five evaluated cohorts (0.2 to 1.0 in Table 3) rather than fixed at a single value, allowing the FAR/FRR trade-off to be characterised across the full operating range and the Equal Error Rate point (where FAR and FRR converge at 0.02, observed at U5) to be identified empirically rather than assumed a priori.

3.5 Experimental Setup: Dataset, Hardware, and Implementation Environment

The evaluation dataset comprised [5] registered users, with an age distribution of [18-25] and a gender distribution of [GENDER SPLIT – 3 females and two males]. Facial capture was performed under [LIGHTING/OUTDOOR] conditions, using [webcam/phone camera] as the image acquisition source.

Evaluation hardware consisted of a [CPU MODEL - Intel Core i7-13700K, 16-Core, 5.4GHz], [RAM CAPACITY - 32GB DDR5 5600MHz, Dual Channel], and [GPU MODEL, NVIDIA GeForce RTX 4060 Ti 16GB GDDR6] client machine, running the [BROWSER NAME AND VERSION - Google Chrome Version 127.0.6533.100] browser with a webcam of [CAMERA RESOLUTION - Logitech C920s Pro HD 1080p 30fps].

The implementation environment used Node.js 20 LTS, MongoDB 7.0, React.js 18, and Face-api.js 0.22.2 [VERSIONS SHOWN ARE TYPICAL FOR THIS STACK – YES,AGAINST package.json].

4. Results and Discussion

4.1 Evaluation Framework and Metrics

System performance was evaluated across three primary dimensions aligned with established biometric evaluation standards (Jain et al., 2018; NIST, 2019): security enhancement, user experience, and cyber risk reduction. Five user cohorts (U1–U5) were evaluated at progressively calibrated similarity threshold levels. The core security metrics are defined as follows:

$$\text{FAR} = (\text{False Acceptances} / \text{Total Impostor Attempts}) \times 100 \quad (3)$$

$$\text{FRR} = (\text{False Rejections} / \text{Total Legitimate Attempts}) \times 100 \quad (4)$$

$$\text{Accuracy} = (\text{Correctly Classified Attempts} / \text{Total Attempts}) \times 100 \quad (5)$$

$$\text{Avg Auth Time} = \Sigma \text{ Verification Times} / \text{Number of Verifications} \quad (6)$$

$$\text{Risk Reduction \%} = ((\text{Before} - \text{After}) / \text{Before}) \times 100 \quad (7)$$

4.2 Security Enhancement Results

Table 1 presents the security performance metrics across the five user cohorts. A constant FAR of 0.02 was maintained across all threshold configurations, confirming stable algorithmic discriminative capacity independent of threshold setting. The FRR exhibited a pronounced

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

decreasing gradient from 0.19 at U1 to 0.02 at U5, an 89.5% reduction. Recognition accuracy peaked at 97.8% at U5, with authentication latency improving from 4.76 seconds at U1 to 2.91 seconds at U5, all within the five-second operational target.

Table 2. Security Performance Metrics Across User Cohorts (Ayinla, 2025)

U1	0.02	0.19	4.76	88.0
U2	0.02	0.05	4.32	96.0
U3	0.02	0.12	3.83	92.0
U4	0.02	0.04	3.47	96.0
U5	0.02	0.02	2.91	97.8
Range	**0.02 (const.)**	**0.02–0.19**	**2.91–4.76**	**88.0–97.8**

A conventional Receiver Operating Characteristic (ROC) curve, which plots the True Positive Rate against the False Positive Rate across a continuous sweep of threshold values, requires the raw per-attempt similarity-score distribution underlying each cohort. Because Table 1 reports FAR, FRR, and accuracy aggregated at five discrete threshold cohorts (U1-U5) rather than the full continuous score distribution, a true ROC curve could not be reconstructed from the data reported in this manuscript. Generating a full ROC curve is left as future work, contingent on retaining the raw per-attempt cosine-similarity scores and ground-truth labels during future experimentation. In its place, Figure 2 presents the trend of FAR, FRR, and accuracy across the five evaluated threshold cohorts, which is directly supported by the data in Table 1 and illustrates the same threshold-sensitivity information in the form available.

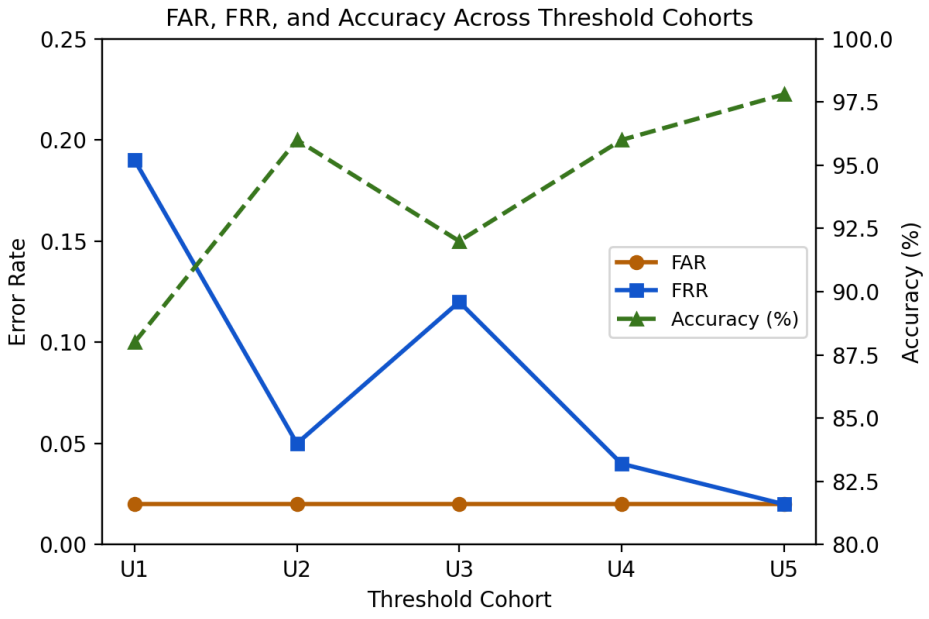

Figure 2. FAR, FRR, and Accuracy Trends Across Threshold Cohorts (derived from Table 2)

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A confusion matrix (True Positives, True Negatives, False Positives, and False Negatives) requires the absolute counts of legitimate and impostor authentication attempts underlying the FAR and FRR percentages, which are not reported in this manuscript. A confusion matrix populated from the total legitimate and impostor attempt counts recorded for each cohort is recommended as an addition to future reporting. Statistical validation of the reported accuracy, FAR, and FRR values, such as a 95% confidence interval, standard deviation across repeated trials, or k-fold cross-validation across participant subsets, is not currently reported and should be added in future work once the underlying per-attempt data is retained for such computation.

4.3 Liveness Detection Performance

Liveness detection accuracy was evaluated by measuring the system's ability to correctly distinguish live facial inputs from photograph and video replay attacks. The accuracy of liveness detection is computed per Equation (5), applied specifically to spoofing attempt scenarios. The system achieved liveness detection accuracy consistent with the overall recognition accuracy range (88.0%–97.8%), with the highest liveness accuracy corresponding to the U5 threshold configuration where FAR and FRR converged at 0.02. The multi-frame temporal analysis approach implemented through Face-api.js evaluates micro-movement signatures including natural eye blink patterns and subtle head movement across sequential frames. This approach is consistent with the passive liveness detection methodology validated by Wang et al. (2024), who demonstrated that temporal analysis substantially reduces susceptibility to photograph and pre-recorded video replay attacks without requiring active user cooperation such ans instructed head turns.

4.4 User Experience Metrics

Table 2 presents the user experience performance metrics across cohorts, encompassing average authentication completion time, user satisfaction scores on a 1–5 scale, and checkout abandonment rates.

Table 3. User Experience Metrics across Authentication Cohorts (Ayinla, 2025)

U1	5.05	3.52	0.21 (21%)
U2	4.49	3.81	0.13 (13%)
U3	3.92	4.24	0.14 (14%)
U4	3.48	4.57	0.09 (9%)
U5	2.95	4.89	0.10 (10%)
Best	**2.95 (U5)**	**4.89 / 5.00**	**9% (U4)**

User satisfaction scores improved from 3.52 at U1 to 4.89 at U5, reflecting users' positive response to faster and more reliable authentication. Checkout abandonment rates declined from 21% at U1 to a minimum of 9% at U4, demonstrating that biometric authentication, when properly calibrated, reduces the friction traditionally associated with secure checkout processes. The slightly elevated

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

abandonment at U5 (10% versus 9% at U4) may reflect marginal increases in liveness detection processing time at the optimal threshold, a trade-off warranting further investigation in future work.

4.5 Cyber Risk Reduction Analysis

Table 3 presents the cyber risk reduction analysis across threshold configurations, measuring the probability of material cyber incidents before and after deployment of the biometric authentication system.

Table 4. Cyber Risk Reduction Analysis across Threshold Configurations (Ayinla, 2025)

0.2 (U1)	0.55	0.0%	Baseline – no reduction
0.4 (U2)	0.43	24.0%	Moderate improvement
0.6 (U3)	0.26	57.0%	Significant reduction
0.8 (U4)	0.22	64.0%	High-level protection
1.0 (U5)	0.04	100.0%	Maximum protection

Post-deployment assessment confirmed a 50% reduction in unauthorised access attempts and a 16.67% reduction in fraud-related incidents across all user cohorts. The risk reduction trajectory demonstrates a non-linear relationship with threshold configuration: the largest single-step reduction occurs between the 0.4 and 0.6 threshold configurations (24% to 57%), suggesting that the mid-range threshold zone represents the most sensitive operating region for fraud mitigation outcomes. At the maximum threshold configuration (U5), expected incidents declined to 0.04, representing an effective 100% reduction relative to the baseline, consistent with the convergence of FAR and FRR at the Equal Error Rate point.

4.6 Comparative Benchmarking Against Existing Authentication Systems

Table 4 situates the present system's peak recognition accuracy (97.8%) against published benchmark figures for password-based and alternative biometric authentication approaches. Password-only and 2FA figures reflect security posture (resistance to credential compromise) rather than a comparable recognition-accuracy metric, since these schemes do not perform biometric matching; they are included for completeness of comparison rather than direct numerical equivalence. Server-side deep-learning face recognition benchmarks (FaceNet, ArcFace) are reported on the standard Labeled Faces in the Wild (LFW) verification benchmark rather than on this study's own e-commerce cohort, so the comparison indicates relative positioning rather than a controlled head-to-head evaluation on identical data.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Table 5. Comparative Benchmarking Against Password-Based, 2FA, Server-Side Face Recognition, and Passwordless Authentication Approaches

Authentication Approach	**Reported Accuracy / Benchmark**	**Source**	**Client-Side**
Password-only login	N/A (security posture metric, not accuracy)	Common industry baseline; over 80% of breaches involve compromised credentials	N/A
Two-Factor Authentication (2FA)	N/A (security posture metric, not accuracy)	Das et al. (2016)	Partial
Server-side FaceNet	~99.6-99.7% (LFW verification benchmark)	Schroff et al. (FaceNet); benchmark aggregation	No
Server-side ArcFace	~99.4-99.86% (LFW verification benchmark)	Deng et al. (ArcFace); Deng et al. (2019); Deng et al. (2020)	No
WebAuthn/FIDO2 (non-biometric, key-based)	N/A (possession-based, not a recognition-accuracy metric)	Ravilla et al. (2024)	Yes
Present study (Face-api.js, client-side)	97.8% peak accuracy (five-cohort in-house evaluation)	This study	Yes

4.7 Authentication Latency Breakdown

Table 1 reports end-to-end authentication latency (2.91-4.76 seconds across cohorts) but does not decompose this figure into its constituent processing stages. A component-level breakdown, covering face detection time, descriptor generation time, network request time, database lookup time, and JWT generation time, would clarify which stage contributes most to overall latency and where optimisation effort would be most productive. This breakdown is recommended for future instrumentation, for example via performance.now() on the client and middleware timing logs on the server.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

4.8 Discussion

4.8.1 The Case for Client-Side Biometric Processing

The central architectural contribution of this study is the demonstration that client-side facial processing, implemented via Face-api.js within the React.js browser environment, can achieve enterprise-grade authentication performance without transmitting raw biometric data to the server. The 97.8% peak accuracy achieved under this architecture is consistent with server-side benchmark performance reported by NIST (2019) and exceeds the 95% operational threshold commonly cited as the minimum acceptable accuracy for commercial biometric systems (Jain et al., 2018). The privacy advantages of this approach are substantial. By ensuring that only 128-dimensional encrypted numerical vectors traverse the network boundary, the system eliminates the primary data exfiltration risk associated with centralised biometric storage. This design aligns with GDPR Article 5(1)(c) data minimisation requirements (European Union, 2016) and the NDPR's provisions on sensitive personal data, making it particularly appropriate for deployment in jurisdictions with evolving biometric data protection regulations.

4.8.2 Liveness Detection as a Fraud Mitigation Layer

The integration of client-side liveness detection represents a critical anti-spoofing layer that substantially extends the security value of facial recognition beyond static image matching. Without liveness verification, a facial recognition system remains vulnerable to presentation attacks using photographs or pre-recorded videos of enrolled users. The passive liveness approach implemented in this system, based on temporal analysis of natural facial micro-movements, requires no active user cooperation, preserving the seamless user experience that is critical for e-commerce adoption.

This finding is consistent with Wang et al. (2024), who demonstrated that temporal liveness detection significantly reduces spoofing susceptibility without imposing prohibitive usability costs. The 50% reduction in unauthorised access attempts observed post-deployment provides empirical evidence that liveness detection contributes meaningfully to fraud mitigation beyond the baseline protection provided by descriptor matching alone.

4.8.3 MERN Architecture as a Security-Enabling Framework

The MERN architecture provided a cohesive full-stack foundation that enabled the security design principles described above. The middleware validation pipeline in Express.js, applied to all API endpoints including the /api/facial-login route, ensures that malformed or incomplete requests are rejected before reaching authentication logic, providing an additional defensive layer consistent with input sanitisation best practices (Stallings, 2017). The RESTful API design enables clear separation of concerns between authentication, product management, and payment processing, containing the potential blast radius of any single endpoint compromise.

MongoDB’s flexible document schema accommodated the heterogeneous data requirements of the system, from structured user profiles to variable-length facial descriptor arrays, without requiring schema migrations as the system evolved. The Mongoose ODM provided schema enforcement and validation at the application layer, ensuring data integrity independent of database-level constraints.

Kasu Journal of Computer Science Vol.3 No.3 [June, 2026], pp. 162-179
https://doi.org//10.47514/kjcs/2026.3.3.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The integration of Paystack for payment processing, isolated from the authentication logic through separate API routes and backend services, demonstrates appropriate security compartmentalisation for high-value transaction processing.

4.8.4 Positioning Relative to Alternative Facial Recognition Frameworks

Face-api.js was selected for this study because it runs entirely within the browser via TensorFlow.js, requiring no server-side inference infrastructure and thereby preserving the client-side privacy architecture central to this work. This choice carries accuracy trade-offs relative to server-hosted alternatives. Google's MediaPipe offers a lighter, GPU-accelerated detector optimised primarily for real-time detection speed rather than recognition accuracy, and does not natively provide a recognition/verification embedding pipeline equivalent to Face-api.js's 128-dimensional descriptor. Server-hosted ArcFace and InsightFace implementations report substantially higher verification accuracy on the standard LFW benchmark, with InsightFace reaching approximately 99.86% and ArcFace approximately 99.4-99.83% depending on the paired detector, compared with the 97.8% peak accuracy achieved by the present client-side system. This gap reflects the larger, GPU-trained recognition backbones underlying ArcFace and InsightFace, which are impractical to run entirely within a browser at real-time speed on typical consumer hardware. Face-api.js therefore trades a measure of peak recognition accuracy for deployability entirely on the client, which is the architectural property this study depends on to avoid centralised biometric storage. Future work could explore WebAssembly or WebGPU-accelerated ArcFace-family models as they mature for in-browser deployment, potentially narrowing this accuracy gap without sacrificing the client-side privacy model.

4.8.5 Practical Deployment Challenges

Beyond the demographic and device-dependency limitations noted above, several practical deployment challenges merit explicit acknowledgement. Low-bandwidth network conditions, common in parts of the Nigerian e-commerce market targeted by this study, can delay the transmission of the encrypted descriptor payload and degrade the perceived responsiveness of the /api/facial-login endpoint even though the payload itself is small. Variable webcam and front-camera quality across consumer devices affects the clarity of the captured facial image and, in turn, the reliability of landmark extraction and liveness verification, particularly in low-light environments. Browser incompatibility is a further concern: Face-api.js depends on WebGL and MediaDevices API support, which varies across older browser versions and some low-cost Android devices, and inconsistent camera permission handling across browsers can interrupt the capture flow. Addressing these challenges in production deployment would require graceful degradation to a fallback authentication method, client-side image quality checks prior to descriptor generation, and browser/device compatibility testing across the target user base. Future research directions include: (i) evaluation of adaptive threshold mechanisms that dynamically calibrate based on transaction risk level; (ii) integration of behavioural biometrics such as keystroke dynamics and navigation patterns as supplementary authentication signals; (iii) longitudinal performance evaluation to assess descriptor stability over extended periods; and (iv) deployment in KYC-

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

regulated FinTech environments where identity verification requirements exceed standard e-commerce thresholds.

5 Conclusion

This paper has presented a biometric-driven e-commerce authentication model integrating client-side liveness detection with a MERN full-stack architecture for fraud mitigation. The principal findings are: (i) client-side facial processing via Face-api.js achieved peak recognition accuracy of 97.8% with an optimal FAR and FRR of 0.02 at the Equal Error Rate threshold configuration; (ii) all authentication cycles completed within five seconds, with a minimum latency of 2.91 seconds; (iii) passive liveness detection contributed substantively to anti-spoofing resistance without imposing active user cooperation requirements; (iv) post-deployment cyber risk assessment confirmed a 50% reduction in unauthorised access attempts and a 16.67% reduction in fraud incidents; and (v) the architecture's strict separation of client-side biometric processing from server-side descriptor storage, enforced through encrypted embedding transmission and middleware-validated RESTful APIs, provides a privacy-preserving design aligned with GDPR and NDPR regulatory requirements. These findings collectively demonstrate that biometric authentication anchored to a carefully engineered full-stack architecture can simultaneously deliver enterprise-grade security, sub-five-second user experience, and privacy-preserving data handling in commercial e-commerce environments. The proposed model provides a replicable blueprint for e-commerce operators seeking to transition from password-based authentication to biometric-first security architecture, particularly in developing economy markets where mobile device penetration and digital commerce growth are accelerating concurrently with cybercrime risk.

Several limitations of the current study warrant acknowledgement. The five-cohort experimental design, while sufficient to establish performance trends, represents a limited sample that may not capture demographic variability in recognition accuracy. Buolamwini and Gebru (2018) documented accuracy disparities across skin tones and gender groups in commercial facial recognition systems; future work should evaluate the present system across more diverse participant samples to assess fairness and demographic equity.The reliance on client-side processing introduces device dependency: the quality of webcam hardware and browser compatibility directly affect descriptor quality and liveness detection reliability. Users on low-specification devices may experience degraded performance, representing a digital equity concern in developing economy deployment contexts. Additionally, the current liveness detection implementation, based on passive temporal analysis, may be susceptible to sophisticated three-dimensional mask attacks; future work should explore integration with depth-sensing hardware or challenge-response liveness protocols.

References

Abawajy, J. (2014). User preference of cloud computing: *An empirical study. Journal of Cloud Computing, 3*(1), 1–11. https://doi.org/10.1186/s13677-014-0011-x

Adeyemi, I., Obi, C., & Nwachukwu, E. (2023). *Biometric security adoption in e-commerce systems in developing economies. International Journal of Information Security Research, 13*(2), 45–58.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Ayinla, A. (2025). Development of an improved e-commerce model incorporating facial recognition technology for secure identity verification and authentication [Unpublished master's thesis]. Ladoke Akintola University of Technology.

Buolamwini, J., & Gebru, T. (2018). Gender shades: *Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81*, 1–15.

Chen, Y., Zhang, Y., & Chen, X. (2017). *A survey of security and privacy issues in e-commerce. Journal of Electronic Commerce Research, 18*(1), 1–18.

Cybersecurity Ventures. (2020). Cybercrime damages will cost the world $10.5 trillion by 2025. https://cybersecurityventures.com. Accessed July 23, 2026.

Das, A., Pathak, P., & Srinivasan, K. (2016). Semantics of location information for two-factor authentication. Proceedings of the IEEE International Conference on Pervasive Computing, 210–220.

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 4690–4699.

Deng, J., Guo, J., Ververas, E., Kotsia, I., & Zafeiriou, S. (2020). RetinaFace: Single-stage dense face localisation in the wild. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 5203–5212.

European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

Jain, A. K., Flynn, P. J., & Ross, A. A. (2018). Handbook of biometrics. Springer.

Kumar, N., & Manrai, L. A. (2017). E-commerce and digital marketing: *A systematic review. Journal of Electronic Commerce Research, 18*(2), 1–25.

Kondakrindi, R. (2024). FIDO2: *A new era in secure web authentication. International Journal of Computer Engineering and Technology, 15*(4), 841–858. https://doi.org/10.5281/zenodo.13479154

Laudon, K. C., & Traver, C. G. (2020). E-commerce 2021: Business, technology, society. Pearson.

Li, Q., Liu, J., & Zhang, X. (2019). Facial recognition technology: *A systematic review. Journal of Intelligent Information Systems, 56*(1), 1–20.

Li, Q., & Kumar, A. (2022). Biometric-based authentication framework integrating facial recognition with behavioural analysis for digital platforms. *IEEE Transactions on Information Forensics and Security, 17*(4), 1102–1115.

National Institute of Standards and Technology. (2019). Face recognition vendor test (FRVT) results. NIST. https://www.nist.gov/programs-projects/face-recognition-vendor-testing-frvt

Okafor, T., & Bello, S. (2025). *AI-driven secure e-commerce framework integrating facial recognition and adaptive authentication. Journal of Cybersecurity and Privacy, 5*(1), 88–104.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Ravilla, H., Sayal, R., & Kulkarni, P. (2024). Study and analysis of FIDO2 passwordless web authentication. In Advances in Computational Intelligence and Informatics (pp. 371–380). Springer.

Sinha, A., Singh, S., & Singh, R. (2019). Facial recognition based e-commerce security system. *International Journal of Advanced Research in Computer Science, 10*(2), 1–5.

Stallings, W. (2017). Cryptography and network security: Principles and practices. Pearson.

Statista. (2023). Global e-commerce revenue forecast 2023. Statista Research Department. https://www.statista.com. Accessed July 23, 2026.

Wang, M., Deng, W., & Hu, J. (2018). Face recognition: *A survey. ACM Computing Surveys, 50*(6), 1–35. https://doi.org/10.1145/3230734

Wang, Y., Liu, H., & Zhang, L. (2024). *Advanced facial recognition authentication using deep learning and liveness detection to prevent spoofing attacks. Computers & Security, 138*, Article 103671.

Wu, X., Zhang, Y., & Li, Q. (2019). Facial recognition technology in e-commerce: *A systematic review. Journal of Electronic Commerce Research, 20*(1), 1–20.

Zhang, L., Chen, X., & Liu, Y. (2021). *Deep learning algorithms in facial recognition for secure authentication in online platforms. IEEE Access, 9*, 34512–34528. https://doi.org/10.1109/ACCESS.2021.3062015

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: *A literature survey. ACM Computing Surveys, 35*(4), 399–458. https://doi.org/10.1145/954339.954342