ORIGINAL RESEARCH PAPER
Volume - 15 | Issue - 04 | April - 2026 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

TRUST: DUAL-FALLBACK BIOMETRIC AUTHENTICATION FOR INCLUSIVE WELFARE DELIVERY IN INDIA'S PUBLIC DISTRIBUTION SYSTEM

Computer Science

Mrs. Balakiruba Assistant Professor, Jansons Institute of Technology
Vimal P B N* UG Student, Jansons Institute of Technology*Corresponding Author
Santhiya A UG Student, Jansons Institute of Technology
Shiba Sri R UG Student, Jansons Institute of Technology
Mohamed Saheem Sees Cheloor Panichiyal UG Student, Jansons Institute of Technology

ABSTRACT

Biometric identity checks now sit at the heart of India's Public Distribution System (PDS), helping to weed out ghost beneficiaries and make sure food goes to the people who actually need it. The hitch? Most ration shops rely only on fingerprint scanning, and that's where things start to break down especially for older folks, manual labourers whose fingerprints have faded over the years, or anyone with disabilities. That means lots of people get left out just because the scanner can't read their prints. Here's where TRUST - Transparent Ration User Security Technology comes in. It's a layered authentication framework with a dual-fallback design. If the Aadhaar fingerprint check flunks, TRUST switches automatically to AI-powered facial recognition using MediaPipe for landmark extraction and cosine similarity for matching. If that step doesn't work either, it moves on to OTP verification via the UIDAI OKYC API, as a last safety net. To make things clearer for rural users who may not read or write well, TRUST walks them through each authentication step with a Tamil-language voice module. Every transaction gets an encrypted, append-only log in the cloud—on Firebase or AWS—so everything's auditable and transparent.Testing TRUST across 500 authentication trials clocked an impressive 99.3% success rate, a whole 16.9 percentage points better than when shops relied solely on fingerprints. The system runs on basic hardware under INR 15,000 and integrates easily with existing setups, thanks to its open-source Python stack (FastAPI, MediaPipe, OpenCV, gTTS, Streamlit).

KEYWORDS

Public Distribution System, Aadhaar Authentication, Facial Recognition, OTP Verification, Biometric Fallback, Cloud Audit Logging

INTRODUCTION

India's Public Distribution System distributes subsidised food grains to over 800 million beneficiaries, making it one of the largest welfare programmes in the world. The integration of Aadhaar-based biometric authentication into ration shops over the past decade has brought measurable improvements in accountability and reduced fraudulent claims. Yet operational evidence from the ground reveals a persistent and significant drawback: fingerprint scanners fail frequently in real-world conditions [1,9]. Ground-level reports from Tamil Nadu ration outlets document between 15 and 20 authentication failures per shop per day, with elderly citizens and manual labourers disproportionately affected due to worn or degraded dermal ridges.

When authentication fails and no fallback exists, ration shop staff face an impossible choice either turn away a legitimate beneficiary or resort to informal distribution, both of which undermine the integrity of the welfare system [1,9]. This paper presents TRUST, a multi-layer authentication platform engineered to eliminate this single point of failure. By deploying AI-based facial recognition and OTP-based verification as structured recovery pathways alongside Tamil voice guidance and tamper-resistant cloud logging TRUST ensures that biometric failure no longer translates into service denial for eligible citizens [3,5].

Advances in lightweight computer vision libraries such as MediaPipe and OpenCV now make real-time facial recognition feasible on standard POS hardware without GPU acceleration. Similarly, the UIDAI OKYC API provides a secure and legally recognised OTP channel that integrates directly with existing Aadhaar infrastructure. This work combines these technologies into a cohesive, deployable framework that preserves backward compatibility with the current PDS authentication workflow while substantially increasing its reliability and inclusivity [4,5,6].

SYSTEM OVERVIEW

TRUST operates as a client-server application in which a Streamlit front-end executes locally on the ration-shop Point-of-Sale (POS) terminal while a Python FastAPI service manages authentication orchestration, inter-module communication, and cloud log dispatch on the backend. The hardware footprint is deliberately minimal: a standard USB fingerprint reader, a consumer-grade webcam (1080p), an audio speaker, and a broadband connection represent the complete physical requirements, ensuring the system can be deployed without capital investment in specialised equipment.

The authentication decision tree operates across three sequential layers. The primary layer invokes Aadhaar fingerprint verification through UIDAI's official API. If the primary layer returns a failure, control passes automatically to the facial recognition module within two seconds. If facial recognition is also inconclusive, the system escalates to OTP-based verification. Only after all three layers are exhausted without a positive match is the session terminated and logged as a verified failure. This cascaded design ensures that transient biometric failures do not permanently block service access for legitimate beneficiaries [1,4,5].

RELATED WORK

Prior studies have examined the limitations of single-modality biometric authentication in government welfare programmes. Jemsala and Shiny [9] documented that digitalization of PDS outlets in Tamil Nadu has exposed persistent authentication gaps, particularly among elderly and semi-literate beneficiaries. Masiero [1] analysed how biometric infrastructure mandates in the Indian PDS inadvertently exclude marginalised communities, arguing that system design must prioritise equitable access alongside security. Pahuja and Goel [5] argued that fairness and reliability must be treated as primary design criteria in any welfare authentication architecture, not secondary considerations after security.

Research on facial recognition as a supplementary biometric has advanced considerably. Jakhete and Kulkarni [3] evaluated MediaPipe Face Mesh comprehensively for real-time facial landmark detection, confirming its suitability for constrained embedded environments directly relevant to PDS deployment. Hayat et et al. [4] demonstrated that combining face and fingerprint recognition through convolutional neural networks yields significantly higher accuracy than any single biometric channel. On multi-modal identity systems, Ammour et al. [7] confirmed that multimodal biometric approaches consistently outperform single-input counterparts in real-world conditions. Salturk and Kahraman [6] validated deep learning-based multimodal authentication integrating facial data for enhanced online security. Faisal et al. [8] analysed time-based one-time password systems, confirming their robustness against replay and interception attacks. Taken together, existing literature confirms both the need for fallback

authentication and the viability of the specific technologies TRUST employs — yet no published system unifies these capabilities within a single PDS-oriented, voice-accessible, audit-transparent platform.

METHODOLOGY

TRUST employs five integrated components to eliminate single-point authentication failure. The primary layer routes fingerprint biometrics through UIDAI's official APIs, maintaining full backward compatibility with existing PDS infrastructure [1,9].

On failure, Fallback Layer 1 activates on-device facial recognition using MediaPipe Face Mesh, tracking 468 facial landmarks and confirming identity at ≥85% cosine similarity — with a local liveness check before any outbound API call [3,7,9]. If still inconclusive, Fallback Layer 2 sends a six-digit OTP (180-second validity) via UIDAI OKYC API; codes void after first use, and three failed attempts auto-terminate the session [8,10].

A Tamil voice module (gTTS) narrates each step as an independent thread, keeping audio guidance active even during exceptions — removing the literacy barrier for rural beneficiaries [1,5]. All events are written to an encrypted cloud audit log (Firebase/AWS, TLS-secured) under an append-only policy, storing six structured fields per transaction to support governance and accountability [2,6,8].

Table 1: Comparison of Existing Aadhaar PDS and Proposed TRUST System

Feature	Existing PDS System	TRUST System
Primary Authentication	Fingerprint only	Fingerprint + Face + OTP
Fallback Mechanism	None	Dual (Face Recognition → OTP)
Accessibility	Text-based interface only	Tamil voice-guided interface
Failure Handling	Service denial to beneficiary	Seamless cascaded fallback
Audit Logging	Minimal transaction records	Encrypted cloud-based logging
Inclusivity	Low for elderly / rural users	High across all beneficiary groups

RESULTS AND DISCUSSION

Evaluation was conducted over 500 staged authentication trials on a standard POS-configured laptop with a USB fingerprint reader and 1080p webcam, spanning eight test conditions including varied lighting, OTP scenarios, and network bandwidths.

TRUST achieved an overall authentication success rate of 99.3%, compared to 82.4% for the fingerprint-only baseline — a net gain of 16.9 percentage points. Facial recognition recovered 14.2% of fingerprint-failed sessions, while OTP verification salvaged a further 7.8%, meaning approximately 97 of every 100 wrongly rejected beneficiaries were successfully served [1,4,9]. Face verification performed strongest under good lighting (97.8% TP rate), with acceptable degradation under dim conditions (88.4%) and partial occlusion (82.6%) [3,7]. Security testing across three adversarial scenarios — photo spoofing, incorrect OTP, and OTP replay — confirmed zero successful breaches [6,8]. Usability observation yielded an aggregate satisfaction score of 4.5/5, with Tamil voice guidance rated highest at 4.7/5, confirming measurable reduction in staff-assisted guidance for elderly and semi-literate users [1,5,9].

Table 2: TRUST System Performance Summary

Module	Success Rate	Avg. Response
Fingerprint	94.6%	1.2 s
OTP Verification	99.3%	4.5 s
Full Fallback Chain	99.3%	11.4 s
Voice Playback	100%	1.0 s
Cloud Audit Log	99.9%	0.8 s

CONCLUSION

This paper presented TRUST, a dual-fallback authentication framework that resolves the documented limitations of fingerprint-only Aadhaar verification in India's Public Distribution System. By deploying AI-based facial recognition and UIDAI OKYC OTP verification as structured recovery layers complemented by Tamil voice guidance for accessibility and encrypted cloud audit logging for accountability TRUST ensures that eligible beneficiaries are not excluded from food entitlements due to biometric hardware failures. Controlled prototype evaluation confirmed an overall authentication success rate of 99.3%, representing a 16.9 percentage-point gain over the fingerprint-only baseline. The system operates on commodity hardware requiring no specialised infrastructure investment, making it viable for large-scale rollout across rural ration outlets. Future development priorities include large-scale field pilots across diverse geographic and demographic settings, integration of anti-spoofing liveness detection, low-bandwidth optimisation for intermittent rural connectivity, and extension to healthcare entitlement, pension disbursement, and subsidy management programmes.

REFERENCES:

[1] S. Masiero, "Biometric Infrastructures and the Indian Public Distribution System," South Asia Multidisciplinary Academic Journal, no. 24/25, 2023.

[2] A. Prabhakar and A. Prakash, "Digital Biometric Authentication and Citizens' Right to Food: Neglect of the Local in India's Aadhaar-enabled Public Distribution System," in Proc. 14th Int. Conf. Theory and Practice of Electronic Governance (ICEGOV), ACM, 2023.

[3] S. A. Jakhete and N. Kulkarni, "A Comprehensive Survey and Evaluation of MediaPipe Face Mesh for Human Emotion Recognition," in Proc. 8th Int. Conf. Communication, Control and Automation (ICCUBEA), IEEE, 2024, doi: 10.1109/ICCUBEA61740.2024.10775188.

[4] A. Hayat et al., "Enhancing Biometric Authentication Through Multimodal Approach Combining Face and Fingerprint Recognition Using Convolutional Neural Networks," Discover Computing, Springer Nature, 2024.

[5] S. Pahuja and N. Goel, "Multimodal Biometric Authentication: A Review," AI Communications, IOS Press, 2024, doi: 10.3233/AIC-220247.

[6] S. Salturk and N. Kahraman, "Deep Learning-Powered Multimodal Biometric Authentication: Integrating Dynamic Signatures and Facial Data for Enhanced Online Security," Neural Computing and Applications, vol. 36, pp. 11311–11322, 2024, doi: 10.1007/s00521-024-09690-2.

[7] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal Approach for Enhancing Biometric Authentication," Journal of Imaging, MDPI, vol. 9, no. 9, p. 168, 2023.

[8] M. Faisal et al., "Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems," International Journal of Computer Technology and Science, vol. 1, no. 3, 2024.

[9] J. Jemsala and S. Shiny, "Perspectives on the Digitalization of Public Distribution System in Kanniyakumari District," Library Progress International, vol. 44, no. 1, 2024.

[10] K. Ashwini et al., "A Novel Multimodal Biometric Person Authentication System Based on ECG and Iris Data," BioMed Research International, vol. 2024, p. 8112209, 2024, doi: 10.1155/2024/8112209.