IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

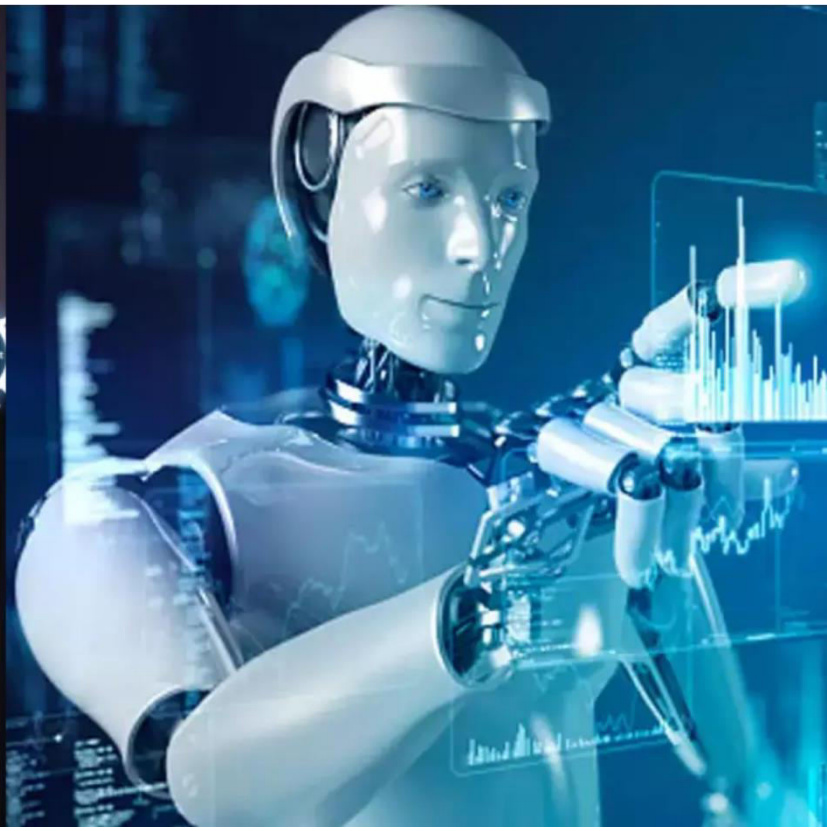
ISSN(O): 2319-8753
ISSN(P): 2347-6710



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Impact Factor: 9.935

Volume 15, Issue 11, November 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511031|

SEAAD Secure Enterprise Attendance and Admin Analytics Dashboard with Passive Liveness Verification

Varry Nohith Kumar, Samudrala Vamshi, Mrs. A. V. Lakshmi Prasuna

U.G. Student, Department of Information Technology, Mahatma Gandhi Institute of Technology, Hyderabad, India

U.G. Student, Department of Information Technology, Mahatma Gandhi Institute of Technology, Hyderabad, India

Assistant Professor, Department of Information Technology, Mahatma Gandhi Institute of Technology, Hyderabad, India

ABSTRACT: Attendance data is useful only when the system can connect an event to the correct employee. Passwords and cards can be shared, while a single face image can be replayed from a photograph or phone. We designed and implemented SEAAD, a workforce management portal that separates password validation from privileged session creation and requires multi-frame facial verification before issuing normal access tokens. The platform combines a React client, an Express and TypeScript application server, PostgreSQL through Prisma, a background worker, and a FastAPI service using InsightFace embeddings. The passive liveness stage examines focus, inter-frame optical flow, motion rigidity, frequency-domain screen artifacts, and cross-frame identity consistency. SEAAD also integrates attendance, leave, departments, tasks, approval workflows, notifications, audit logging, and workforce analytics. Five scenario-based acceptance tests documented for biometric check-in, spoof rejection, role enforcement, leave approval, and automatic absence marking completed with the expected functional outcome. These tests establish feature behavior but do not replace a controlled biometric benchmark; population-level APCER, BPCER, false-acceptance, and false-rejection measurements remain future work.

KEYWORDS: Attendance security, passive liveness detection, face verification, role-based access control, JWT revocation, workflow automation, workforce analytics.

I. INTRODUCTION

Attendance records influence payroll, compliance, resource planning, and disputes about physical presence. Their value depends on the integrity of the identity event that creates them. Passwords, personal identification numbers, and access cards prove possession or knowledge, but they do not prove that the legitimate employee is physically present. This weakness enables proxy attendance and credential delegation. A facial verifier improves identity binding, yet a single image can be vulnerable to printed photographs or images replayed on another display.

SEAAD addresses this problem as an integrated system rather than as an isolated recognition model. Credential validation produces only a short-lived provisional token whose purpose is restricted to biometric completion. The server grants normal role-bearing access only after the face service accepts a multi-frame sample. The same platform maintains attendance, leave, departments, tasks, approval workflows, notifications, and analytical views, allowing authentication decisions and administrative events to share a consistent authorization and audit model.

We built the project around five practical objectives: prevent password-only access from becoming a normal privileged session; reject simple photographic and screen presentations before accepting a face match; preserve one attendance record per employee and date; automate approvals and background attendance work; and give each organizational role a focused view of operational data. The contribution is therefore the integration and enforcement of these mechanisms, not the training of a new face-recognition network. A controlled study is still required before making population-level biometric accuracy claims.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511031|

II. RELATED WORK

A. Facial representation and verification

FaceNet demonstrated that metric learning can map faces to a representation in which distance reflects identity similarity [1]. ArcFace improved class separation by adding an angular margin during training [2]. SEAAD uses the InsightFace implementation with the compact buffalo_sc model package, which combines an SCRFD-family detector with an ArcFace-family embedding model. The project consumes a pretrained representation; its contribution is the surrounding verification, liveness, session, and enterprise-control architecture rather than a newly trained facial network.

B. Presentation attack detection

ISO/IEC 30107-3 defines evaluation concepts for presentation attack detection, including attack and bona fide error rates [3]. Prior work has explored learned depth, texture, and central-difference representations [4], [5]. SEAAD instead implements a CPU-oriented passive ensemble using classical image and temporal signals. The design is intended for ordinary webcams and therefore avoids an active user challenge or specialized depth sensor. This engineering choice reduces interaction cost but cannot provide the guarantees of a dedicated three-dimensional sensor.

C. Access control and token lifecycle

Role-based access control associates permissions with organizational roles [6], while JSON Web Tokens provide signed, portable claims [7]. A signed token normally remains valid until expiry unless the verifier consults additional state. SEAAD keeps access tokens short-lived and validates a per-user version when a refresh token is redeemed. Logout increments that version, invalidating previously issued refresh tokens without requiring a per-token blacklist.

III. SYSTEM ARCHITECTURE

SEAAD is a modular monolith with an independent inference service and worker process. The React single-page application communicates with the Express API through REST and receives notification events through Server-Sent Events. Express applies security headers, credentialed origin checks, rate limits, JSON limits, bearer-token verification, and role authorization before dispatching requests to domain modules. Prisma maps these modules to PostgreSQL. The separate Node worker runs scheduled attendance, workflow, task, analytics, and outbox jobs. The FastAPI service is reached through multipart HTTP for face enrollment, verification, quality analysis, landmarks, and similarity operations.

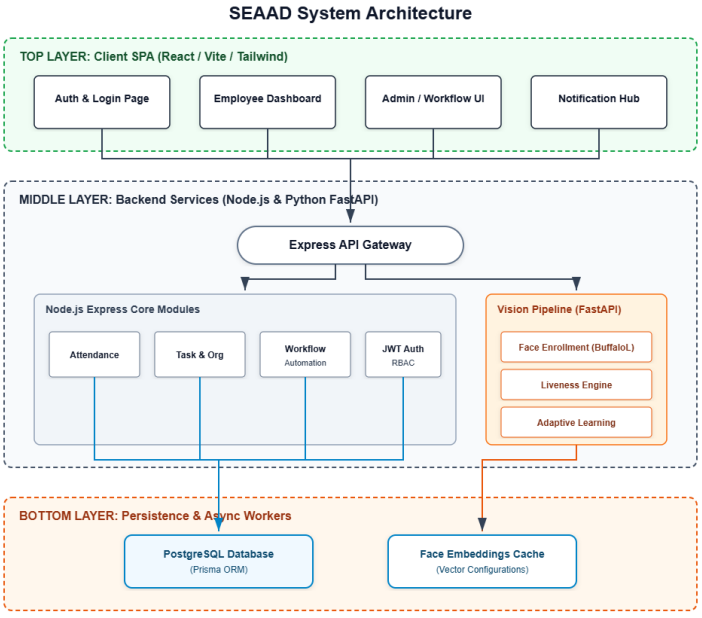


Fig. 1. Layered SEAAD architecture. Face embeddings are persisted in PostgreSQL as employee profile data; the diagram's cache label represents the logical embedding store rather than a separate vector database.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511031|

Layer	Implemented technology	Primary responsibility
Presentation	React 18, TypeScript, Vite	Authentication, dashboards, attendance, administration, tasks and analytics
Application	Express 5, TypeScript	REST API, validation, JWT enforcement, RBAC and domain orchestration
Inference	FastAPI, InsightFace, ONNX Runtime, OpenCV	Enrollment, liveness, embedding fusion and verification
Persistence	PostgreSQL 15, Prisma	Identity, attendance, organization, workflow, tasks, notifications and audit data
Asynchronous	Node worker, node-cron, transactional outbox	Escalation, reminders, anomaly processing and reliable side effects

TABLE I. IMPLEMENTED PLATFORM LAYERS

IV. PROPOSED METHOD

A. Two-phase identity-bound authentication

Let Tprov denote a provisional JWT whose purpose claim is 2FA_PENDING. After validating email and a bcrypt password, the login endpoint returns only Tprov. Authentication middleware rejects this token on normal protected routes and accepts it only through middleware dedicated to enrollment, verification, or the configured fallback path. Following successful facial verification, the server creates a 15-minute access token Tacc and a seven-day refresh token Tref. The refresh token is carried in an HttpOnly cookie; the browser holds Tacc in memory and attaches it as a bearer credential.

Each user stores tokenVersion v(u). Tref contains the version that existed at issuance. During refresh, the server verifies the signature, loads the user, and requires the token version to equal v(u). Logout increments v(u), so older refresh tokens can no longer mint a new access token. Already issued access tokens remain valid until their short expiry, which is an explicit limitation of the design rather than instantaneous revocation of every request.

B. Enrollment and multi-frame representation

Enrollment accepts one to five images and stores one or more normalized embeddings in the employee record. Verification requires at least two uploaded frames in the current implementation. Images are decoded, resized, normalized, and evaluated for basic quality. Valid face detections produce 512-dimensional representations. Multi-frame verification fuses the available representations and compares the probe against the stored gallery using cosine distance. Successful high-confidence probes may update the bounded gallery when the adaptive-learning diversity rule accepts them.

C. Passive liveness gate

The current liveness decision is conjunctive for the signals that participate in the final gate. Image focus is measured through Laplacian variance. Farneback optical flow requires non-zero inter-frame motion. A rigidity test estimates whether motion directions are excessively uniform, as expected from a planar object. A two-dimensional Fourier transform over the facial region measures anomalous high-frequency peaks associated with screen recapture. Cross-frame embedding consistency prevents a sequence containing different identities from being accepted. Eye-aspect-ratio variance is calculated when landmarks permit it, but the present two-frame flow treats the blink result as informational rather than mandatory.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511031|

Signal	Implemented role	Decision status
Laplacian focus	Rejects blurred or unusable captures	Mandatory early gate
Optical flow	Requires temporal motion between frames	Mandatory
Motion rigidity	Rejects strongly planar directional motion	Mandatory
FFT screen artifacts	Detects high-frequency recapture peaks	Mandatory
Cross-frame consistency	Checks that frames represent one identity	Can override acceptance
Eye dynamics	Measures landmark-based variance	Informational in current flow

TABLE II. LIVENESS AND CONSISTENCY SIGNALS IN THE CURRENT IMPLEMENTATION

D. Enterprise transaction and analytics model

Attendance records use a composite unique constraint over user and date, preventing duplicate daily rows even when concurrent requests bypass an application-level pre-check. Leave approval can create or update attendance state through a transaction. Departments support unlimited nesting through a parent relation and materialized path. The workflow engine separates reusable templates from runtime instances and steps, while the task engine records assignments, status updates, comments, and due dates. Notifications are persisted and distributed to connected clients through SSE; an outbox records side effects that are retried asynchronously. Scheduled jobs mark absences, escalate workflows, detect anomalies, refresh analytical views, and send task reminders.

V. FUNCTIONAL EVALUATION

A. Enforcement properties supported by the repository

Table III distinguishes implementation-backed enforcement from experimental claims. These properties are established by route composition, middleware ordering, token payloads, schema constraints, and service call sequencing. Runtime behavior still requires integration testing against a disposable database and inference service before publication as an empirical result.

Property	Implementation evidence	Boundary
Password alone does not mint normal access	Login returns only a 2FA-purpose token	Fallback-login policy must be evaluated separately
Provisional token cannot access normal protected routes	Authentication middleware blocks purpose 2FA_PENDING	Depends on every sensitive route using the middleware
Role restrictions are server-side	authorize middleware checks req.user.role	Role-to-business-scope rules vary by module
Refresh sessions are revocable	Refresh payload carries tokenVersion; logout increments it	Current access token survives until its 15-minute expiry
Duplicate daily attendance is constrained	Unique userId and date index in PostgreSQL schema	Requires deployed migrations to match the schema
Face overwrite from provisional login is blocked	Enrollment controller rejects overwrite under a 2FA-purpose token	Administrative re-enrollment remains privileged functionality
Outbox work is retryable	Events store status, attempts and availableAt	Delivery channels must be idempotent under retries

TABLE III. REPOSITORY-SUPPORTED SECURITY AND RELIABILITY PROPERTIES

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511031|

B. Deployment and operational structure

Docker Compose defines PostgreSQL, the face service, the Express API, a separate worker, and an Nginx-hosted frontend. The API container applies Prisma migrations before startup. Development scripts run the API, worker, face service, and Vite client in separate processes. GitHub Actions installs Node dependencies, generates Prisma Client, runs the backend checks, lints and builds the frontend, and performs Python syntax checks. At the time of analysis, the CI face command still referenced a deleted face_pipeline.py file, so the workflow requires correction before it can serve as reproducible evidence.

C. Scenario-based acceptance testing

We evaluated the integrated application through five end-to-end scenarios selected from the main security and administrative paths. Each scenario defined an input, expected behavior, and observed functional outcome. The observations were recorded during project testing and are summarized in Table IV. They show that the exercised workflows reached their intended states; they do not measure recognition accuracy across a representative population.

Test scenario	Expected system behavior	Documented outcome
Live biometric check-in	Accept a live multi-frame sample, verify identity, and create PRESENT attendance	Expected check-in flow completed
Photograph or phone presentation	Fail liveness and create no attendance record	Presentation was rejected and attendance was blocked
Employee opens administrator routes	Redirect in the client and return HTTP 403 from protected APIs	Client and server role checks blocked access
Manager approves sick leave	Approve request, update balance, and record an audit event	Leave state and balance were updated
No check-in by day boundary	Scheduled worker creates an ABSENT record for eligible employees	Automatic absence processing completed

TABLE IV. SCENARIO-BASED FUNCTIONAL TEST OUTCOMES RECORDED IN THE PROJECT DOCUMENTATION

D. Biometric evaluation still required

The acceptance tests are useful for checking integration, but a research-grade biometric evaluation requires genuine and impostor trials across subjects, sessions, lighting, pose, and capture devices. Presentation attacks should include printed photographs and several display technologies. ISO/IEC 30107-3-aligned reporting should include APCER and BPCER; identity verification should additionally report false acceptance, false rejection, equal error rate, ROC/AUC, and confidence intervals. Ablation experiments should compare single-frame verification, optical-flow-only liveness, and the complete implemented gate.

VI. LIMITATIONS AND THREATS TO VALIDITY

Passive two-dimensional analysis cannot reliably reject every virtual-camera replay or three-dimensional mask. A recorded sequence of a bona fide person may satisfy motion and consistency checks unless capture freshness is cryptographically challenged. The current eye-dynamics result is not part of the mandatory pass condition, and using only two frames limits temporal evidence. Thresholds are implementation parameters rather than population-calibrated operating points. Adaptive gallery updates may reduce rejection under appearance drift but also introduce template-poisoning risk unless updates are carefully monitored and reversible.

The system also has operational limitations. The face service has no independent service-to-service credential and should remain on a private network. SSE authentication places an access token in the query string, which may expose it to logs. Several task and workflow actor identifiers are strings rather than database foreign keys. Email delivery is a stub. Cron schedules inherit the worker's local timezone. Finally, the current automated suite covers only a small set of

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511031|

backend helper functions and does not establish end-to-end correctness, authorization completeness, biometric accuracy, or deployment availability.

The privacy impact is material because facial embeddings and workforce behavior are sensitive. A deployment requires informed consent, retention rules, encryption and access controls, an accessible non-biometric recovery process, bias monitoring, incident response, and compliance review. The architecture should not be interpreted as eliminating the need for organizational governance.

VII. CONCLUSION AND FUTURE WORK

SEAAD demonstrates how identity verification, session lifecycle, attendance integrity, and enterprise administration can be combined in one working application. Its principal design decision is to delay normal role-bearing token issuance until a multi-frame liveness and face-verification step succeeds. Versioned refresh tokens, database constraints, transactional outbox processing, hierarchical departments, workflows, tasks, and anomaly detection extend this trust boundary beyond the login screen. The five recorded acceptance scenarios exercised the principal biometric, authorization, leave, and scheduling paths successfully. Quantitative biometric and performance claims nevertheless remain subjects for controlled evaluation.

Future work should add challenge-bound capture freshness, service authentication for the inference tier, CIDR-aware network policy, confidential biometric storage, reversible adaptive updates, stronger foreign-key coverage, timezone-explicit scheduling, and comprehensive integration tests. The next research phase should calibrate thresholds and evaluate APCER, BPCER, false acceptance, false rejection, latency, resource consumption, and demographic consistency on an ethically collected dataset.

REFERENCES

[1] F. Schroff, D. Kalenichenko, and J. Philbin, 'FaceNet: A unified embedding for face recognition and clustering,' in Proc. IEEE CVPR, 2015, pp. 815-823.
[2] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, 'ArcFace: Additive angular margin loss for deep face recognition,' in Proc. IEEE/CVF CVPR, 2019, pp. 4690-4699.
[3] ISO/IEC 30107-3:2017, Information technology - Biometric presentation attack detection - Part 3: Testing and reporting, 2017.
[4] Z. Yu et al., 'Searching central difference convolutional networks for face anti-spoofing,' in Proc. IEEE/CVF CVPR, 2020, pp. 5295-5305.
[5] Y. Liu, A. Jourabloo, and X. Liu, 'Learning deep models for face anti-spoofing: Binary or auxiliary supervision,' in Proc. IEEE/CVF CVPR, 2018, pp. 389-398.
[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, 'Role-based access control models,' Computer, vol. 29, no. 2, pp. 38-47, 1996.
[7] M. Jones, J. Bradley, and N. Sakimura, JSON Web Token (JWT), RFC 7519, IETF, 2015.
[8] J. Guo, J. Deng, A. Lattas, and S. Zafeiriou, 'Sample and computation redistribution for efficient face detection,' in Proc. ICLR, 2022.
[9] Z. Boulkenafet, J. Komulainen, and A. Hadid, 'Face anti-spoofing using color texture analysis,' IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1232-1244, 2016.
[10] G. Bradski, 'The OpenCV Library,' Dr. Dobb's Journal of Software Tools, 2000.
[11] OWASP Foundation, 'OWASP Application Security Verification Standard 4.0.3,' 2021.
[12] PostgreSQL Global Development Group, 'PostgreSQL 15 Documentation: Constraints,' 2022.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details