Yellow Sense Technologies Pvt Ltd

Startup India - Govt of India DP - IIT: DIPP – 138 388 | MSME Udyog Aadhar: UDYAM-KR-03-0293956

CIN: U-62099-KA-2023-PTC-174648 | PAN: AABCY6908P | TAN: BLRY02955B

+91 9869.397.868, +91 9284.367.406 | prakhar@yellowsense.in | https://yellowsense.in

Startup name: YellowSense Technologies Pvt. Ltd.

Incubator Name: IIIT-Bangalore Innovation Center (Dr Lakshmi and Natarajan Sir)

Grant received (Rs 7 lakhs) from: Govt of INDIA - MEITY TIDE 2.0 – Oct 2025

Challenge: Face Liveness Detection (UIDAI – SITAA Program), ID: SU-C1-2025-01 | **Date:** 18th Jan 2026

1. OVERALL PROPOSAL SUMMARY:

We propose a 6-month, stage-wise development of an AI-based Face Liveness Detection system, progressing from PoC to pre-commercial readiness (**TRL 3 → TRL 8**), fully aligned with UIDAI SITAA challenge timelines and deliverables. The proposed **₹2.5 crore** budget covers **end-to-end R&D and pre-commercial readiness over 6 months**, strictly aligned to Stage 1–4 milestones defined by UIDAI SITAA.

Duration: 6 Months
Total budget asked for: INR 2.5 crore
TRL Progression: TRL-3 → TRL-8

1. 1 Problem Being Addressed

1. Face-based biometric systems are vulnerable to:
    - Printed photograph attacks
    - Video replay attacks
    - Mask-based impersonation
    - Synthetic / deepfake media
2. Existing active-only liveness systems:
    - Increase user friction
    - Cause authentication drop-offs
    - Remain vulnerable to trained attackers
3. UIDAI requirements demand:
    - Low-friction user experience
    - High spoof detection accuracy
    - Real-time inference
    - Edge compatibility across enrolment and authentication devices

1.2 Core Solution Concept

1. Hybrid liveness detection system

2. Passive liveness as default decision path
3. Active liveness triggered only when confidence is low
4. Implemented as an SDK, independent of UI
5. Designed for:
    - Enrolment systems (desktop / webcam)
    - Authentication systems (both mobile / handheld and desktop / webcam).

The system combines passive liveness as default (texture, depth, rPPG, optical-flow, frequency cues) with active liveness as fallback, and an explicit deepfake/digital attack detection layer.

All inference is on-device by default, secured using TEE / hardware-backed keystore, with zero biometric persistence.

1.3 End-to-End Technical Workflow

1. Video / camera input capture (short unprompted clip)
2. Face detection and cropping
3. Passive liveness analysis
    - Motion consistency
    - Texture stability
    - Temporal coherence
4. Confidence score generation
5. Decision branching:
    - Score ≥ threshold → LIVE
    - Score < threshold → Active liveness
6. Active liveness verification (blink-based)
7. Final LIVE / SPOOF decision

1.4 Execution Plan:

Stage-wise delivery aligned to UIDAI SITAA timelines, with strict focus on technology development.

Working Demo (Basic PoC - Proof of Concept):

https://github.com/yellowsense2008/YellowSense_FaceLiveness_Detection

https://yellowsense.in

The current work represents an early TRL-2+ implementation, where a basic end-to-end face liveness detection processing pipeline has been validated in controlled conditions. This existing prototype will be systematically matured into a robust, UIDAI-compliant TRL-3 PoC during Stage-2 of the program.

Hence, the Stage-2 TRL-3 PoC will be **significantly more advanced** than the current baseline prototype, with quantitative benchmarking, dataset-driven validation, and SDK-grade stability.

Final Outcome:
A pre-commercial, scalable, and privacy-preserving face liveness detection solution suitable for national digital identity systems.

---

2. STAGE-WISE TIMELINE & DELIVERABLES

Stage 1 – Project Design Document (PDD)

Timeline: T0 + 1 Month
Funding Allocation: 20% = INR 50 lakhs

Key Activities

- Final system architecture (passive-first + active fallback)
- Spoof taxonomy (print, replay, mask, deepfake, adversarial)
- Dataset finalization (UIDAI + India-representative augmentation)
- Evaluation plan aligned to **ISO/IEC 30107 & UIDAI APCER/BPCER**
- SDK integration blueprint (enrolment + auth flows)

Deliverables

- PDD (architecture, models, security, metrics)
- Dataset & evaluation protocol
- Risk & mitigation plan

Stage 2 – Proof of Concept (PoC | TRL 3)

Timeline: T0 + 2 Months
Funding Allocation: 20% = INR 50 lakhs

Stage-2 focuses on **maturing the existing early PoC** into a **fully validated TRL-3 SDK**, strengthening robustness across acquisition variability, demographic diversity and reproducibility under UIDAI-defined evaluation protocols.

Key Activities

- Passive liveness baseline (CNN-ViT texture, depth, motion cues)
- Initial deepfake / replay detection module
- Single-device prototype (Android reference)
- Baseline benchmarking on UIDAI sandbox datasets

Deliverables

- Working POC pipeline
- Initial accuracy & latency report
- Demonstration on enrolment + authentication scenarios

Stage 3 – MVP (Beta Release | TRL 6)

Timeline: T0 + 4 Months
Funding Allocation: 30% = INR 75 lakhs

Key Activities

- Passive + active hybrid fusion (active only on low confidence)
- rPPG stabilization and low-light robustness
- Deepfake robustness (RGB + optical-flow fusion)
- On-device optimization (TFLite / ONNX, INT8/FP16)
- Secure inference via **TEE / Android Keystore**

Deliverables

- Android SDK (Beta)
- Liveness score + spoof class + confidence output
- Performance reports (APCER / BPCER / latency)
- Integration documentation

Stage 4 – MRP (Pre-Commercial | TRL 8)

Timeline: T0 + 6 Months
Funding Allocation: 30% = INR 75 lakhs

Key Activities

- Model hardening & final calibration
- UIDAI sandbox integration testing
- Device & environment matrix validation
- Security audit, DPDP compliance pack
- Deployment & handover documentation

Deliverables

- Production-ready SDK (MRP) | Scalability testing (Aadhaar-scale simulations)
- ISO/IEC 30107-aligned evaluation report
- Security hardening and audit readiness
- Integration readiness with UIDAI systems | Final technical documentation.

FINAL Output:
Pre-commercial solution ready for deployment and certification.

3. REVISED BUDGET STATEMENT

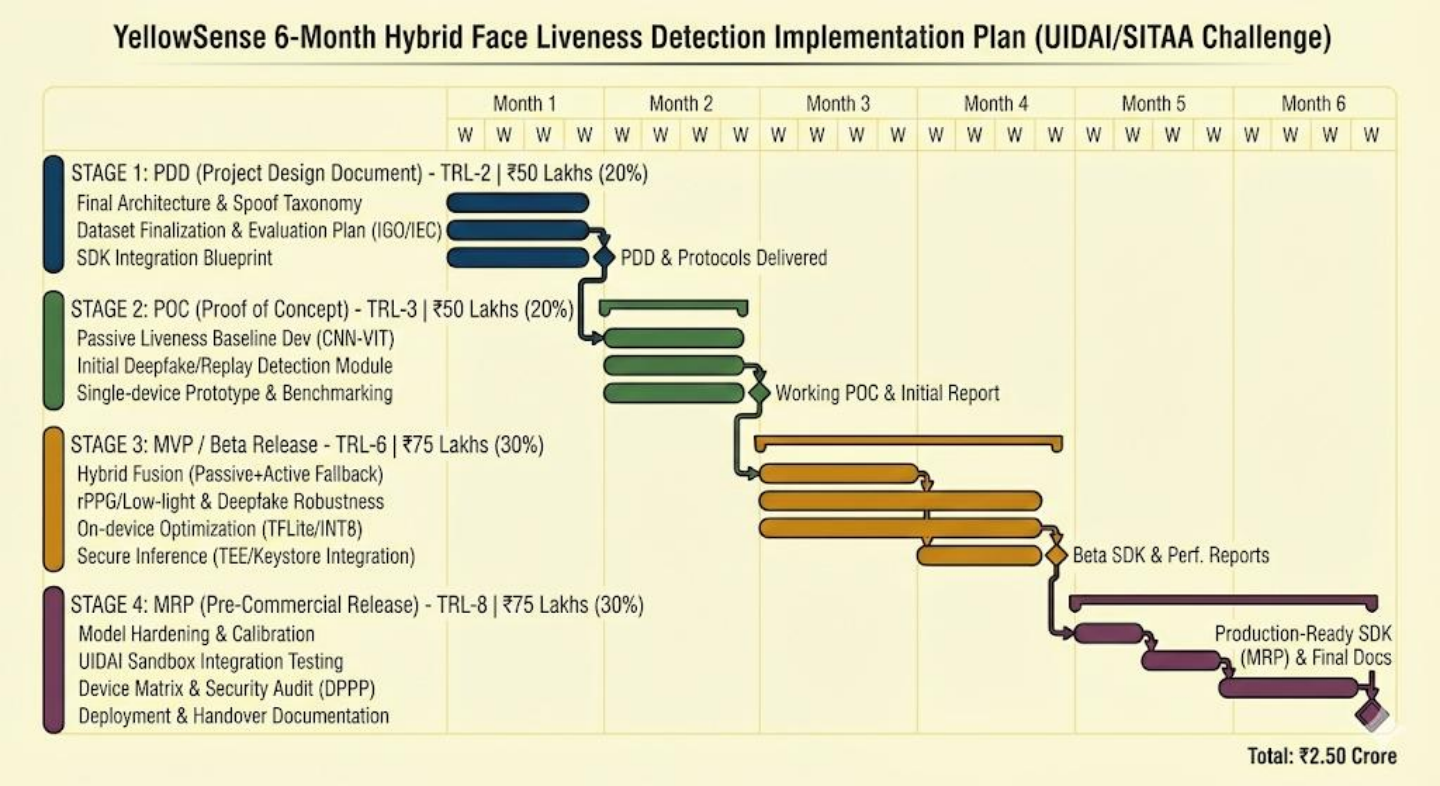
The total project budget (INR 2.5 crore) is strictly aligned to a 6-month execution window and allocated stage-wise as per SITAA guidelines: Stage 1 – 20%, Stage 2 – 20%, Stage 3 – 30%, Stage 4 – 30%.

Stage	Timeline	%	Amount (₹)	Objective and Deliverables
Stage 1 – PDD	T0+1 month	20%	₹50 lakh	Final architecture, datasets, evaluation plan
Stage 2 – PoC (TRL-3)	T0+2 months	20%	₹50 lakh	Working liveness + spoof detection prototype
Stage 3 – MVP (TRL-6)	T0+4 months	30%	₹75 lakh	SDK-ready, optimized, secure on-device system
Stage 4 – MRP (TRL-8)	T0+6 months	30%	₹75 lakh	Pre-commercial, UIDAI-ready release
Total	**6 months**	**100%**	**₹2.5 crore**	

The budget is exclusively focused on:

- AI/ML model development | Dataset collection and annotation
- SDK and system engineering | Security and performance validation

Gantt Diagram:



4. REVISED TECHNICAL SOLUTION & TECHNICAL ARCHITECTURE:

4.1 System Architecture (SDK-Based)

Core Modules

1. Frame Processor
    - Frame extraction
    - Normalization
    - Sequence preparation
2. Face Detector
    - Face localization
    - Valid face region enforcement

3. Passive Liveness Model
    - Motion features
    - Texture consistency
    - Temporal analysis
4. Active Liveness Module
    - Blink detection using EAR
    - Landmark tracking across frames
    - Time-bound challenge execution
5. Decision Engine (SDK Core)
    - Passive + active score fusion
    - Threshold-based classification

4.2. Passive Liveness Detection (Primary)

1. No explicit user prompts
2. Uses natural facial behavior
3. Input:
    - Short unprompted video
4. Feature extraction:
    - Micro facial movements
    - Texture continuity
    - Temporal coherence
5. Model:
    - Lightweight CNN
6. Output:
    - Liveness confidence score [0–1]
7. Optimized for:
    - Real-time inference
    - CPU-only execution
    - Edge devices

4.3. Active Liveness Detection (Fallback)

1. Triggered only when passive confidence is below threshold
2. Used in:
    - Poor lighting
    - Low-quality cameras
    - Borderline confidence cases
3. Technique:
    - Blink detection
    - Eye Aspect Ratio (EAR)
    - Facial landmark temporal validation
4. Security:
    - Randomized timing
    - Replay-resistant challenges
5. Objective:
    - Strengthen final decision
    - Minimize friction for genuine users

4.4. Hybrid Decision Logic

1. Passive score evaluated first
2. If passive score ≥ threshold:
    - User marked LIVE
3. If passive score < threshold:
    - Active liveness triggered
4. Final decision based on:
    - Passive confidence
    - Active challenge outcome

4.5. Performance & Optimization Strategy

1. Real-time liveness detection
2. Low-latency inference suitable for authentication
3. Optimization techniques:
    - Lightweight CNN architecture
    - Limited frame window
    - Efficient preprocessing and batching
    - CPU-only inference

4. Edge readiness:
    - Desktop enrolment systems
    - Mobile authentication devices
    - Minimal memory footprint
    - Stable across lighting and environments

4.6. Security, Privacy & Compliance

4.6.1 Security Measures

1. Detection of:
    - Photo attacks
    - Video replay attacks
    - Mask-based impersonation
2. Hybrid liveness reduces spoof success
3. Active fallback prevents static attacks

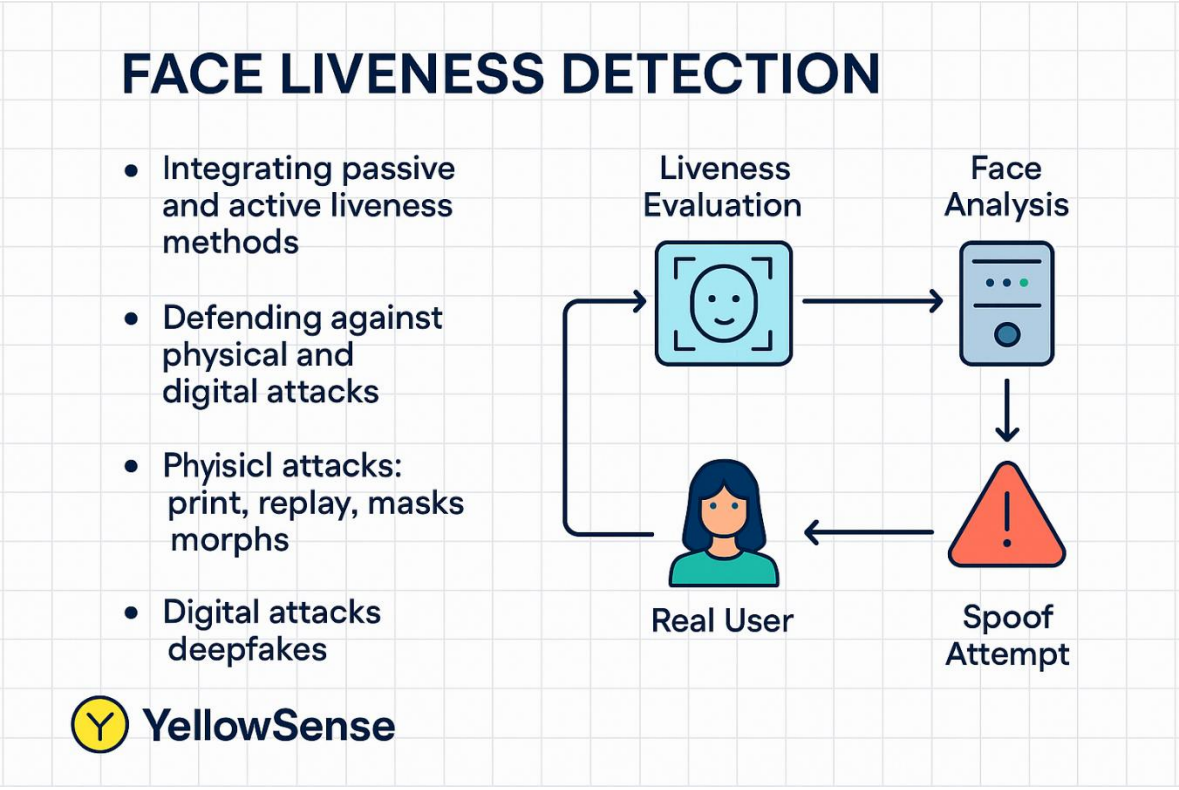
4.6.2 Privacy-Preserving Design

1. No biometric data stored permanently
2. All processing performed locally
3. No dependency on external cloud services
4. Privacy-by-design architecture

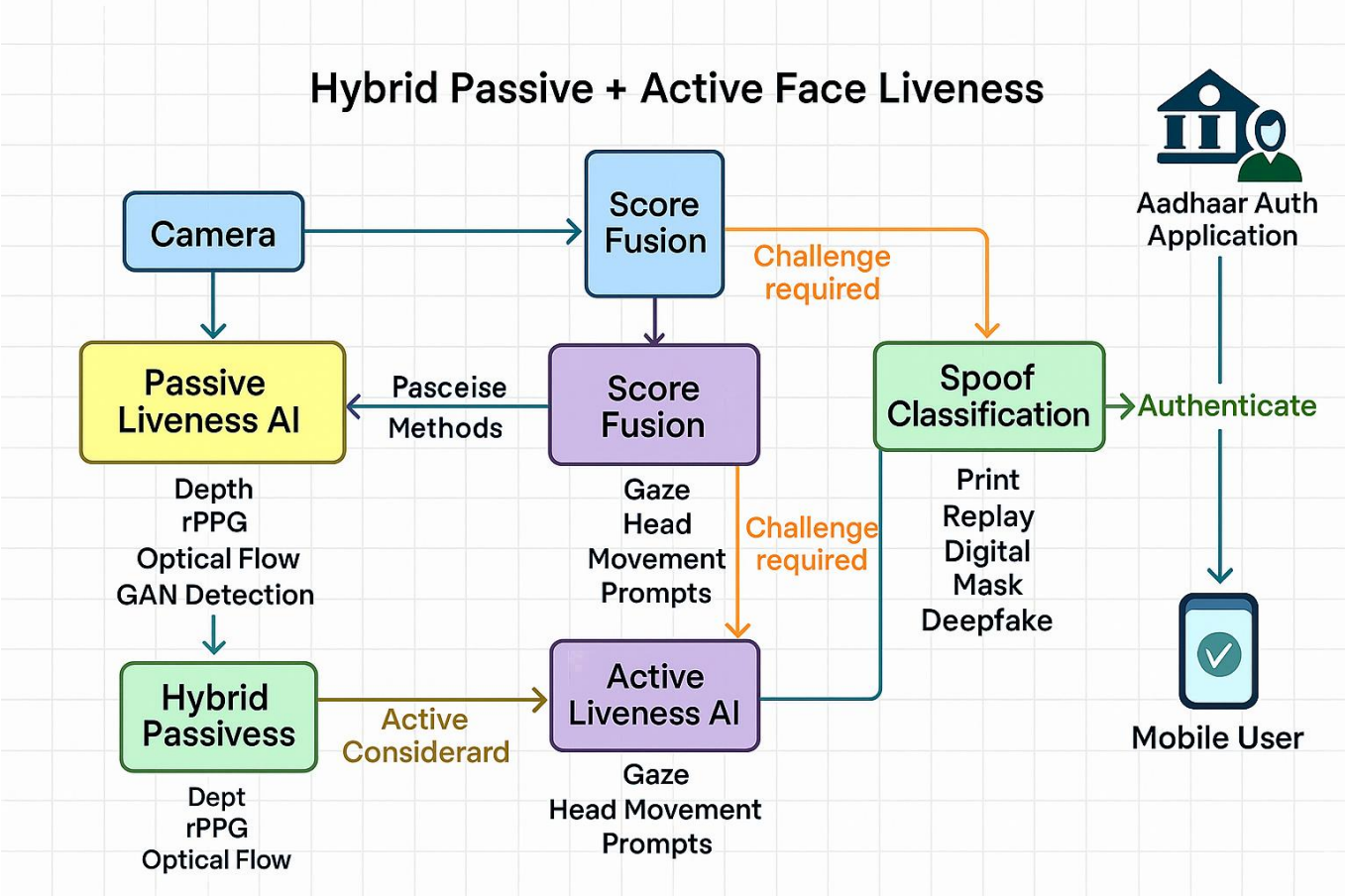
4.6.3 Compliance Alignment

1. Aligned with ISO/IEC 30107 (PAD)
2. Designed for UIDAI enrolment workflows
3. Designed for UIDAI authentication workflows

Block diagram:



Architecture Diagram (Face Liveness Detection)



5. AI/ML MODEL BUILDING CAPABILITIES, PAST RELEVANT EXPERIENCE & EVIDENCE OF UNDERSTANDING CONTACTLESS FINGER BIOMETRICS:

5.1. Identity & Face Biometric AI Systems (Relevant Experience)

- Built and prototyped **AI-based face identity and liveness verification systems** involving:
  - Face detection, alignment, and normalization
  - Passive and active face liveness detection
  - Presentation attack detection (PAD) for enrolment and authentication flows
- Developed **end-to-end computer vision pipelines** operating on:
  - Low-resolution webcam feeds (enrolment)
  - Mobile RGB camera streams (authentication)
  - Short video sequences under uncontrolled lighting and pose
- Experience handling **real-world biometric data challenges**, including:
  - Motion blur, compression artifacts, illumination variance
  - Partial face visibility and framing inconsistencies
  - Device and camera heterogeneity
- Hands-on exposure to **cross-device and cross-environment variability**, which is a core challenge in Aadhaar face authentication at national scale.

5.2. Face Liveness & Anti-Spoofing Expertise

- Designed **hybrid face liveness detection pipelines** combining:
  - Passive liveness (motion, texture, temporal consistency)
  - Active liveness (blink-based challenge–response as fallback)
- Experience detecting a wide range of **presentation attacks**, including:
  - Printed photo attacks
  - Video replay attacks
  - Mask-based impersonation
  - Synthetic / deepfake facial media
- Applied **temporal modeling and texture-based feature extraction**, such as:
  - Micro-movement analysis across frames
  - Texture stability checks to detect recapture artifacts
  - Landmark-based temporal validation for active challenges
- Clear understanding that **liveness systems must balance**:
  - Security and spoof resistance
  - User friction and authentication drop-offs
  - Latency constraints for real-time authentication
- Experience aligning **AI outputs with regulator-grade trust requirements**, not just ML accuracy metrics.

5.3. Large-Scale, Sensitive Biometric Data Handling

- Prior work on **AI systems in government and regulated environments**, where:
  - Biometric data sensitivity is high
  - Auditability and traceability are mandatory

- Familiarity with **privacy-first biometric system design**, including:
  - No permanent biometric storage
  - Local, on-device processing wherever possible
  - Minimal data retention and controlled telemetry
- Understanding of **biometric dataset governance**, including:
  - Consent-aware data handling
  - Secure preprocessing pipelines
  - Dataset lifecycle management aligned to regulatory expectations
- Experience building systems where **privacy-by-design is a core architectural requirement**, not an afterthought.

5.4. Model Development & Optimization Experience (Face Biometrics)

- Trained and evaluated **deep learning models for face analysis**, including:
  - CNN-based feature extractors
  - Lightweight temporal models for video-based inference
- Experience optimizing models for:
  - Low-latency inference suitable for authentication use-cases
  - CPU-only execution on edge devices
  - SDK-based deployment rather than cloud-only pipelines
- Practical exposure to:
  - Frame window optimization to reduce compute load

    - Efficient preprocessing and batching strategies
    - Stability across diverse lighting and camera conditions
- Demonstrated ability to:
    - Transition from research-grade models
    - To deployable, integration-ready SDK components.

5.5. Readiness for UIDAI Face Liveness Detection Challenge

- Clear understanding of **UIDAI-specific face liveness challenges**, including:
    - Minimizing user friction during authentication
    - Supporting both enrolment and authentication workflows
    - Operating reliably across India-scale demographic and environmental diversity
- Proposed solution directly addresses:
    - Passive-first liveness to reduce drop-offs
    - Active fallback only in low-confidence scenarios
    - Edge compatibility for enrolment PCs and mobile devices
- Capability to:
    - Design datasets and evaluation protocols
    - Benchmark against APCER/BPCER-style error metrics
    - Deliver measurable improvements within a **6-month, stage-gated SITAA framework**
- Strong continuity from prior biometric and identity AI work to **face PAD–specific system design**.

---

6. FEASIBILITY, SCALABILITY, AND TECHNICAL SOUNDNESS (FACE LIVENESS)

- Implementation structured into **clearly defined, time-bound stages**:
    - PDD → PoC → MVP → MRP
    - Fully aligned to the 6-month SITAA challenge framework
- Modular **SDK-based architecture** enables:
    - Rapid iteration of liveness models
    - Independent improvement of passive and active components
    - Integration without redesigning enrolment or authentication systems
- Designed for **India-scale deployment**, supporting:
    - Desktop-based enrolment setups
    - Mobile-based authentication devices
    - Consumer-grade cameras without specialized hardware

- Uses **industry-standard, well-tested AI frameworks**, ensuring:
    - Stability
    - Maintainability
    - Ease of audit and validation
- Architecture supports future extensions to:
    - Advanced PAD techniques
    - Multi-modal biometrics (face + other signals)
    - Deeper integration with Aadhaar ecosystem components
- Technical risks mitigated through:
    - Stage-wise validation and reviews
    - Progressive performance benchmarking
    - Controlled expansion from PoC to pre-commercial readiness

7. TRACTION / ONGOING CUSTOMERS:

- **IIIT Bangalore (P3Dx):** Homomorphic encryption + consent AI project – MOU signed.
- **New Mangaluru Port:** Maritime cargo forecasting intelligence – MOU in progress.
- **Stellantis:** OT anomaly detection + PLC bypass detection (active discussions – NDA signed, factory visit done) – computer vision, image processing, video analytics, AI/ML.
- **Kerala Government:** Welfare fraud anomaly detection demoed – AI/ML.
- **RBI Harbinger Cybersecurity:** Bharat-Trust AI Platform selected for round-2.

8. TEAM MEMBERS:

Key Founders

1. Prakhar Goyal — Founder, CEO & CTO

   • Qualification: B.Tech + M.Tech, Computer Science, IIT Bombay

   • Experience: Ex-Microsoft, Amazon, SAP; 15+ yrs in large-scale AI/ML data platforms, cybersecurity solutions, forensics authentication using distributed systems and machine learning models, LLMs, NLP.

   • Role: Leads AI architecture, cybersecurity systems, product engineering.
   • Email: prakhar@yellowsense.in | 9869397868
   • LinkedIn: https://www.linkedin.com/in/prakhar-goyal-1744021b/

2. Komal Goyal — Co-Founder & COO

   • Qualification: BCom, MBA; 8+ yrs experience in operations, customer engagement, field deployments.
   • Role: Drives operations, partnerships, execution at customer sites.
   • Email: komal@yellowsense.in | 9284367406
   • LinkedIn: https://www.linkedin.com/in/komal-goyal-51b09555/

Technology Team:

1. Ms Binita Mahto – Senior AI/ML Engineer
   • Qualification: MSc – Computing and Mathematics, IIT Dhanbad
   • Role: Leads the AI/ML development and drives the performance optimisation of the LLM models.
   Email: binita@ai.yellowsense.in
   https://www.linkedin.com/in/binita-mahto-b491a020b/

2. Abhimanyu Malik — Senior AI/ML Engineer
   • Qualification: B.Tech, Thapar Institute of Technology
   • Role: Builds real-time detection systems, secure AI pipelines, & high-performance model deployment.

   Email: abhimanyu@ai.yellowsense.in
   https://www.linkedin.com/in/abhimanyu-malik-19190622a/

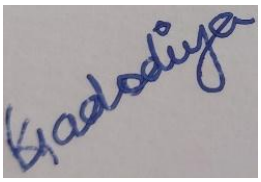
3. Dweep Solanki – CyberSecurity & AI/ML Engineer
   • **Qualification:** BSc in CyberSecurity, Siliguri Institute of Technology
   • **Role:** AI/ML systems development, AI pipelines, computer vision, cybersecurity anomaly detection.

   Email: dweep@ai.yellowsense.in
   https://www.linkedin.com/in/dweep-solanki/

4. Animesh Sharma — AI Engineering Intern
   • **Qualification:** B.Tech (final year), IIT Patna
   • **Role:** AI/ML systems development, AI pipelines, computer vision, cybersecurity anomaly detection.
   Email: animesh@ai.yellowsense.in
   https://www.linkedin.com/in/animesh-sharma-144732250/

5. Talha Nagina – AI/ML Intern
   • **Qualification**: BTech, Nirma University
   • **Role:** Deals with the datasets and pre-processing/fine-tuning of the models using Kaggle/open source.
   Email: talha@ai.yellowsense.in
   https://www.linkedin.com/in/talhanagina306/

Yours Faithfully,



Name: Ms Komal Goyal & Mr Prakhar Goyal
Designation: Directors at Company (CHRO and CTO)
Date: 18th Jan 2026

CERTIFICATE NO:
DIPP138388

#startupindia

Government of India
Ministry of Commerce & Industry
Department for Promotion of Industry and Internal Trade

CERTIFICATE OF RECOGNITION

This is to certify that ***YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED*** *incorporated as a* ***Private Limited Company*** *on* ***07-06-2023****, is recognized as a startup by the Department for Promotion of Industry and Internal Trade. The startup is working in 'House-Hold Services' Industry and 'Home Care' sector as self-certified by them.*

This certificate shall only be valid for the Entity up to **Ten** years from the date of its incorporation only if its turnover for any of the financial years has not extended ₹ **100 Cr.**

11-07-2023	06-06-2033
DATE OF ISSUE	VALID UPTO

INNOVATE KARNATAKA

K-tech

ಕರ್ನಾಟಕ ಸರ್ಕಾರ

GOVERNMENT OF KARNATAKA

ಎಲೆಕ್ಟ್ರಾನಿಕ್ಸ್, ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಮತ್ತು ಜೈವಿಕ ತಂತ್ರಜ್ಞಾನ ನಿರ್ದೇಶನಾಲಯ

DIRECTORATE OF ELECTRONICS, INFORMATION TECHNOLOGY & BIOTECHNOLOGY

ನೋಂದಣಿ ಪ್ರಮಾಣಪತ್ರ

REGISTRATION CERTIFICATE

ಮೆ|| YELLOW SENSE TECHNOLOGIES PRIVATE LIMITED ಸಂಸ್ಥೆಯು 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY, PINNACLE HEIGHTS, Dr. Shivarama Karanth Nagar, Bangalore North, Bangalore - 560077, Karnataka, Bengaluru, Karnataka - 560077-' ವಿಳಾಸದಲ್ಲಿ ನೋಂದಾಯಿತ ಕಛೇರಿಯನ್ನು ಹೊಂದಿದ್ದು 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY, PINNACLE HEIGHTS, Dr. Shivarama Karanth Nagar, Bangalore North, Bangalore - 560077, Karnataka, Bengaluru, Karnataka - 560077' ಸ್ಥಳದಲ್ಲಿರುವ ಘಟಕವನ್ನು 'ಸ್ಟಾರ್ಟ್‌ಅಪ್' ಎಂದು ಕರ್ನಾಟಕ ಸ್ಟಾರ್ಟ್‌ಅಪ್ ಪಾಲಿಸಿಯನ್ವಯ ನೋಂದಾಯಿಸಲ್ಪಟ್ಟಿದ್ದು, ಈ ಕೆಳಕಂಡಂತೆ ನೋಂದಣಿ ಸಂಖ್ಯೆಯನ್ನು ನೀಡಲಾಗಿದೆ.

having its Registered Office at the address: 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY, PINNACLE HEIGHTS, Dr. Shivarama Karanth Nagar, Bangalore North, Bangalore - 560077, Karnataka, Bengaluru, Karnataka - 560077' is registered as a 'Startup' with the 'Karnataka Startup Cell' for the unit located at the 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY, PINNACLE HEIGHTS, Dr. Shivarama Karanth Nagar, Bangalore North, Bangalore - 560077, Karnataka, Bengaluru, Karnataka - 560077' and has been allotted the Registration Number as given hereunder:

The certificate shall only be valid for the entity.

* Up to 10 years from the date of its incorporation/registration of the Company.

ಸಂಖ್ಯೆ: ಕಿಟ್ಸ್/ಎಸ್ ಕೆ-ನೋಂದಣಿ/2023-24/3086
No: KITS/SK-REGN/2023-24/3086
Incorporation Date: 07-06-2023

ದಿನಾಂಕ/Date: 01-01-2024
ಸ್ಥಳ: ಬೆಂಗಳೂರು
Place: Bengaluru

ಸಿಸ್ಟಮ್ ವಿಶ್ಲೇಷಕ (ಡಿಇಐಟಿ) ಮತ್ತು ಪ್ರಧಾನ ವ್ಯವಸ್ಥಾಪಕರು (ಐಟಿ) ಕಿಟ್ಸ್
System Analyst (DEIT) & General Manager (IT) KITS
ಬಿಎಂಟಿಸಿ ಕಟ್ಟಡ, 'ಬಿ'ಬ್ಲಾಕ್, 4ನೇ ಮಹಡಿ, ಕೆ.ಎಚ್ ರಸ್ತೆ, ಬೆಂಗಳೂರು-560027
BMTC Building, 'B'Block, 4th Floor, K.H Road, Bengaluru-560027

सत्यमेव जयते

GOVERNMENT OF INDIA
MINISTRY OF CORPORATE AFFAIRS

Central Registration Centre

Certificate of Incorporation

[Pursuant to sub-section (2) of section 7 and sub-section (1) of section 8 of the Companies Act, 2013 (18 of 2013) and rule 18 of the Companies (Incorporation) Rules, 2014]

I hereby certify that YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED is incorporated on this SEVENTH day of JUNE TWO THOUSAND TWENTY THREE under the Companies Act, 2013 (18 of 2013) and that the company is Company limited by shares

The Corporate Identity Number of the company is **U62099KA2023PTC174648**

The Permanent Account Number (PAN) of the company is **AABCY6908P***

The Tax Deduction and Collection Account Number (TAN) of the company is **BLRY02955B***

Given under my hand at Manesar this SEVENTH day of JUNE TWO THOUSAND TWENTY THREE

Certification signature by DS MINISTRY OF CORPORATE AFFAIRS 10 <roc.cro@mca.gov.in> Validity Unknown
Digitally signed by DS MINISTRY OF CORPORATE AFFAIRS 10
Date: 2023.06.10 10:31:31 IST

PM Mohan

Assistant Registrar of Companies/ Deputy Registrar of Companies/ Registrar of Companies

For and on behalf of the Jurisdictional Registrar of Companies

Registrar of Companies

Central Registration Centre

Disclaimer: This certificate only evidences incorporation of the company on the basis of documents and declarations of the applicant(s). This certificate is neither a license nor permission to conduct business or solicit deposits or funds from public. Permission of sector regulator is necessary wherever required. Registration status and other details of the company can be verified on mca.gov.in

Mailing Address as per record available in Registrar of Companies office:

YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED

F N0 9C LAVENDER REGENCY,PINNACLE HEIGHTS,Dr. Shivarama Karanth Nagar,Bangalore North,Bangalore-560077,Karnataka

*as issued by Income tax Department

Office address: IIIT Bangalore Innovation Center, 1st Floor, Ramanujan Block, IIIT Bangalore campus, Electronic City Phase 1, Bengaluru - 560100, Karnataka, India.

Registered corporate addr: F N0 9-C, Lavender Block, Regency Pinnacle Heights, Rachaenahalli, Dr. SRK Nagar, Bengaluru, KA-560077