ScanPoint: A Real-Time ID Detection system using ML

Submitted in partial fulfilment of the requirements of the degree of

BACHELOR OF ENGINEERING

by

Ankit Pawar: 22106135

Mohit Rajput: 22106126

Harsh Salunkhe: 22106133

Jay Wadnere: 22106105

Guide:

Prof. Shubham Zanwar

Department of Computer Science & Engineering

(Artificial Intelligence & Machine Learning)

A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

(2025-2026)

A.P. SHAH INSTITUTE OF TECHNOLOGY, THANE

CERTIFICATE

This is to certify that the project entitled **"ScanPoint: A Real-Time ID Detection system using ML "** is a bonafide work of **Ankit Pawar (22106135), Mohit Rajput (22106126), Harsh Salunkhe (22106133), Jay Wadnere (22106105)** submitted to the University of Mumbai in partial fulfilment of the requirement for the award of the degree of **Bachelor of Engineering** in **Computer Science & Engineering (Artificial Intelligence & Machine Learning).**

Prof. Shubham Zanwar
Guide

Prof. Sayali P. Badhan
Project Coordinator

Prof. Dr. Jaya Gupta
Head of Department

Dr. Uttam D. Kolekar
Principal

A.P. SHAH INSTITUTE OF TECHNOLOGY, THANE

Project Report Approval for B.E.

This project report entitled **“ScanPoint: A Real-Time ID Detection system using ML”** by **“Ankit Pawar(22106135), Mohit Rajput(22106126), Harsh Salunkhe(22106133),Jay Wadnere(22106105)”** is approved for the degree of ***Bachelor of Engineering*** in ***Computer Science & Engineering (Artificial Intelligence & Machine Learning), 2025-26***.

Examiner Name   Signature

1.__________________   ______________

2.___________________   _______________

Date:

Place:

Declaration

We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Ankit Pawar & 22106135)

(Mohit Rajput & 22106126)

(Harsh Salunkhe & 22106133)

(Jay Wadnere & 22106105)

Date:

Abstract

Identity verification plays a crucial role in security, banking, e-governance, and access control systems. Traditional manual methods for ID verification are time-consuming, error-prone, and susceptible to fraud. In this work, we present a real-time identity detection system using machine learning that automates the process of identifying and verifying identity documents. The proposed framework integrates image preprocessing, feature extraction, and classification models to accurately detect and analyze ID cards in diverse real-world conditions. Convolutional Neural Networks (CNNs) are employed to learn discriminative visual features from identity cards, while optical character recognition (OCR) techniques are incorporated for extracting textual information. The system is designed to handle variations in lighting, orientation, and document quality, ensuring robustness during live detection. Two operational modes are explored: a classification approach for verifying document authenticity and an object detection approach for locating key ID regions such as photos, names, and numbers. This work contributes to reducing manual verification effort, enhancing security, and enabling integration in applications such as KYC processes, border security, and fraud prevention.

Keywords:

Real-Time ID Detection, Machine Learning, Computer Vision, Convolutional Neural Network (CNN), Optical Character Recognition (OCR), Identity Verification

SDG Goals:

SDG 9: Industry, Innovation, and Infrastructure

SDG 16: Peace, justice, and strong Institutions

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF GRAPHS

ABBREVATION

Abbreviation	Full Form
OCR	Optical Character Recognition
CNN	Convolutional Neural Network
SNN	Siamese Neural Network
ID	Identity Document
API	Application Programming Interface

Chapter 1

Introduction

Identity verification is an essential process in modern digital and physical ecosystems, ensuring security, trust, and compliance across multiple domains such as banking, government services, travel, and corporate access control. Traditional methods of ID verification often rely on manual inspection, which is not only time-consuming but also prone to human error and fraudulent manipulation. With the increasing prevalence of identity theft and document forgery, there is a growing need for automated, accurate, and real-time solutions that can reliably authenticate identity documents.

Recent advancements in machine learning and computer vision have opened new opportunities for automating ID detection and verification. By leveraging deep learning models such as Convolutional Neural Networks (CNNs), systems can be trained to recognize complex visual patterns and textual information from identity cards under diverse environmental conditions. These models can detect key components of an ID card, including the photograph, name, ID number, and security features, while handling variations in orientation, lighting, and image quality.

The objective of this project is to design and implement a real-time ID detection system using machine learning that ensures speed, accuracy, and robustness. The proposed system combines image preprocessing, feature extraction, and classification techniques to enable efficient document recognition. By integrating Optical Character Recognition (OCR) with deep learning-based object detection, the framework not only validates document authenticity but also extracts critical information for downstream verification tasks.

Furthermore, the project introduces face verification mechanisms by comparing the photograph on the ID card with a live/selfie capture of the individual. This biometric layer of verification significantly strengthens the reliability of the system by ensuring that the document holder and the document owner are the same person. Advanced preprocessing techniques such as illumination normalization, denoising, and quality assessment enhance face recognition accuracy even under challenging conditions like low light or motion blur.

The system also incorporates database integration for cross-referencing ID numbers and validating against authoritative records, enabling the classification of documents as "legit," "fake," or "unknown." This multi-layered approach—combining OCR, text parsing, database lookup, and biometric face matching—provides a comprehensive verification pipeline suitable for both governmental security use cases and commercial applications such as KYC (Know Your Customer) in banking, fraud prevention in insurance, and secure access in corporate environments.

Looking forward, the integration of transformer-based models (Vision Transformers, BERT for OCR text) and generative adversarial networks (GANs) for forgery detection can further enhance robustness against sophisticated fraud attempts. In addition, deploying the system on edge devices such as mobile phones or kiosks would enable real-time, on-device verification without depending entirely on cloud infrastructure, ensuring scalability, privacy, and accessibility.

Thus, this project stands at the intersection of machine learning, biometrics, and security, offering a scalable, automated, and intelligent framework for next-generation identity verification.

In addition, the proposed framework addresses one of the critical challenges of modern ID verification systems—balancing accuracy with efficiency. While deep learning ensures high precision in feature extraction and matching, optimized preprocessing and lightweight models make the system suitable for real-time deployment. The inclusion of dynamic thresholding for face similarity and error correction mechanisms in OCR ensures adaptability across diverse input conditions. The system's modular design also allows for easy extension to other document types such as passports, voter IDs, and employee badges. By combining multiple layers of validation—text, database lookup, and biometric matching—the solution provides a multi-factor verification approach that is far more resilient to fraud than traditional methods. Ultimately, this project aims to contribute toward a secure, scalable, and intelligent digital identity infrastructure that meets the demands of today's security-driven world.

Chapter 2

Literature Survey

Year	Title	Domain	Algorithm	Dataset	Gap
2024	IDTrust: Deep Identity Document Quality Detection with Bandpass Filtering	ID document quality assessment	Deep CNN with bandpass filtering	MIDV-2020, L3i-ID	Focuses on document quality (original vs scanned) but not full real-time ID detection or information extraction.
2024	First Competition on Presentation Attack Detection on ID Card (PAD-IDCard)	Presentation attack detection (anti-spoofing)	Multiple ML/DL models (competition setting)	Sequestered dataset from 4 countries	Provides benchmarking, but no unified model; dataset not publicly available, limiting reproducibility.
2025	Identity Documents Recognition and Detection Using Semantic Segmentation with CNN	Real-time ID document detection	Semantic Segmentation with CNN	Custom dataset (synthetic + real ID samples)	Optimized for resource-constrained devices, but needs evaluation on diverse global ID formats and larger datasets.
2023	Attention Enhanced Siamese Neural Network for Face Validation	Face verification / matching	Siamese neural network + attention mechanism	Small-scale face pair	Focuses on few-shot face data; not specific to ID cards domain

2023	Fake Face Detection in Identity Cards Using Stegoface	ID card face manipulation detection	Steganography + CNN for face manipulation in ID cards	ID card face datasets (MRTD)	Focused on face only, not full document OCR or field parsing.
2024	Application and analysis of face matching based on the Siamese model in face recognition	Face matching / verification	Siamese model applied in face recognition context	Face recognition datasets (not specified for ID)	Face-matching focused but lacks specific consideration of ID-card/selfie and field extraction pipeline.
2023	Deep Learning Based Face Recognition Method using Siamese Network	Face recognition	Siamese network (VGG encoder) in an unsupervised manner	Unspecified face image dataset (unlabeled)	General face recognition rather than ID-document face matching.
2024	Enhancing OCR Accuracy for ID-1 Documents with Security Features through Machine Learning-driven Image Optimization	ID cards with security features	ML-driven image preprocessing + OCR	ID-1 format documents with security features (e.g., driving license)	Focused on image optimisation rather than full field extraction or matching; may not cover cross-document verification.

Chapter 3

Limitations of Existing Systems

Limitations of Existing ID Verification Approaches

1. Manual / Traditional Verification

- Time-consuming and labor-intensive, requiring significant manpower.
- Highly subjective, as decisions vary between human operators.
- Prone to fatigue-related errors when dealing with large volumes of documents.
- Inefficient for high-throughput environments (airports, banks, large-scale government programs).
- Fraud detection is weak, as subtle forgeries (micro-texts, hologram tampering) often escape manual inspection.

2. Rule-Based / Template-Matching Systems

- Relies on fixed layouts and predefined templates, which fail when ID card designs change.
- Cannot handle diverse ID formats across regions/countries (e.g., driving licenses vary even within a single country).
- Struggles with orientation issues (tilted/scanned images), poor lighting, and low-quality captures from mobile cameras.
- Lack of scalability—each new ID format requires manual template updates, slowing adoption.

3. Basic OCR-Based Systems

- Sensitive to noise, distortions, shadows, and partial occlusions in scanned/captured IDs.
- High error rates when extracting text from complex backgrounds, watermarks, or holograms.
- Fails in multi-language settings where IDs may contain multiple scripts (e.g., Hindi + English in India).
- Cannot validate authenticity of extracted data (only reads the text, but cannot detect if numbers are forged/manipulated).
- Limited ability to perform contextual corrections (e.g., distinguishing between “O” and “0”).

4. Existing Automated Solutions

- Many AI-based solutions lack the real-time processing speed required for live verification at checkpoints.
- Focus mainly on either textual data (OCR) or visual features (photo/logo), but rarely combine both effectively.
- Vulnerable to spoofing attacks (e.g., presenting photocopies, screenshots, or replayed digital images).
- Systems often fail against adversarial attacks, where forged IDs are designed to trick OCR/AI models.
- Deployment challenges: high computational cost, requiring cloud GPUs, making them less feasible for on-device/edge verification.

5. General Observations

- The problem remains unsolved: scalability, robustness, and strong anti-fraud mechanisms are still open research challenges.
- Current solutions are usually domain-specific, tailored for one country or document type, lacking global adaptability.
- Regulatory compliance (GDPR, RBI KYC norms, etc.) is often overlooked in automated solutions, limiting adoption.
- Lack of explainability—systems act as "black boxes," making it difficult for authorities to justify decisions in legal/regulatory contexts.

Chapter 4

Problem Statement, Objectives and Scope

Problem Statement:

Identity verification is a critical requirement in various domains such as banking, e-governance, travel, corporate security, and online services. Traditional methods rely on manual inspection or rule-based systems, which are time-consuming, error-prone, and vulnerable to fraud. With the increasing sophistication of identity theft, forgery, and spoofing attacks, conventional approaches are no longer sufficient.

Existing automated solutions, such as basic OCR engines or template-matching techniques, often fail under real-world conditions such as:

- Poor lighting and background noise.
- Variations in document orientation and quality (e.g., tilted scans, blurred mobile captures).
- Diverse ID card formats across regions and countries.
- Forged or tampered IDs with manipulated text, photos, or holograms.

These limitations highlight the need for a robust, scalable, and real-time identity verification system that combines computer vision, deep learning, OCR, and biometric validation to achieve high accuracy and resilience against fraud.

Objectives:

The primary objective of this project is to design and implement a machine learning-based framework for real-time identity document detection and verification. Specifically, the system aims to:

- Design a robust image processing pipeline using advanced preprocessing methods (grayscale conversion, denoising, thresholding, morphological operations) to enhance ID card features.
- Apply deep learning models (e.g., CNNs, ResNet50-based Siamese networks) for detecting and extracting key components such as the photograph, name, date of birth, and ID number.
- Integrate OCR techniques (Tesseract with configurable PSM/OEM) for reliable extraction of textual information across different ID formats.
- Implement intelligent error correction to address common OCR issues (e.g., confusing O with 0, I with 1).
- Ensure robust performance under real-world conditions, including variations in orientation, lighting, blur, and environmental noise.
- Incorporate face verification using biometric matching between the ID card photo and a live/selfie capture of the user.
- Enable database integration for real-time cross-verification of ID numbers and detection of fraudulent records.
- Provide scalability for practical applications, including KYC processes, corporate access control, border security, e-governance, and fraud prevention.
- Maintain modularity so that the framework can be easily extended to support multiple document types (passports, driver’s licenses, voter IDs, employee badges).

Scope:

The project focuses on building an intelligent, automated, and modular system for real-time ID detection and verification. The scope of the system includes:

- Development of a machine learning pipeline that integrates image preprocessing, OCR, and deep learning-based face verification.
- Support for multiple image formats (JPG, PNG, JPEG, WEBP) captured via cameras, scanners, or mobile devices.
- Deep learning-based detection models (CNN/ResNet50) capable of generalizing across diverse ID formats, fonts, and languages.
- Integration of OCR (Optical Character Recognition) for accurate extraction of text attributes such as Name, ID Number, Date of Birth, and Address.
- Testing and benchmarking the system under varied real-world scenarios, including poor lighting, skewed angles, blurred images, and partial occlusions.
- Face verification pipeline using preprocessing (alignment, normalization, CLAHE, noise reduction) and a Siamese network with ResNet50 backbone for high-accuracy matching.
- Dynamic thresholding and quality checks to minimize false positives and negatives in biometric matching.
- Database validation through PostgreSQL/Supabase for detecting fake IDs and verifying document authenticity.
- Scalability and modularity—designed for deployment in real-world applications such as:
  - Banking and financial KYC processes.
  - Government e-governance and public service authentication.
  - Corporate access management.
  - Border control and immigration verification.
  - Fraud detection in insurance, rentals, and e-commerce.
- Future extensibility: Incorporation of advanced deep learning methods (ArcFace, Vision Transformers, GAN-based forgery detection) and deployment on edge/mobile devices for offline verification.

Chapter – 5

Proposed System

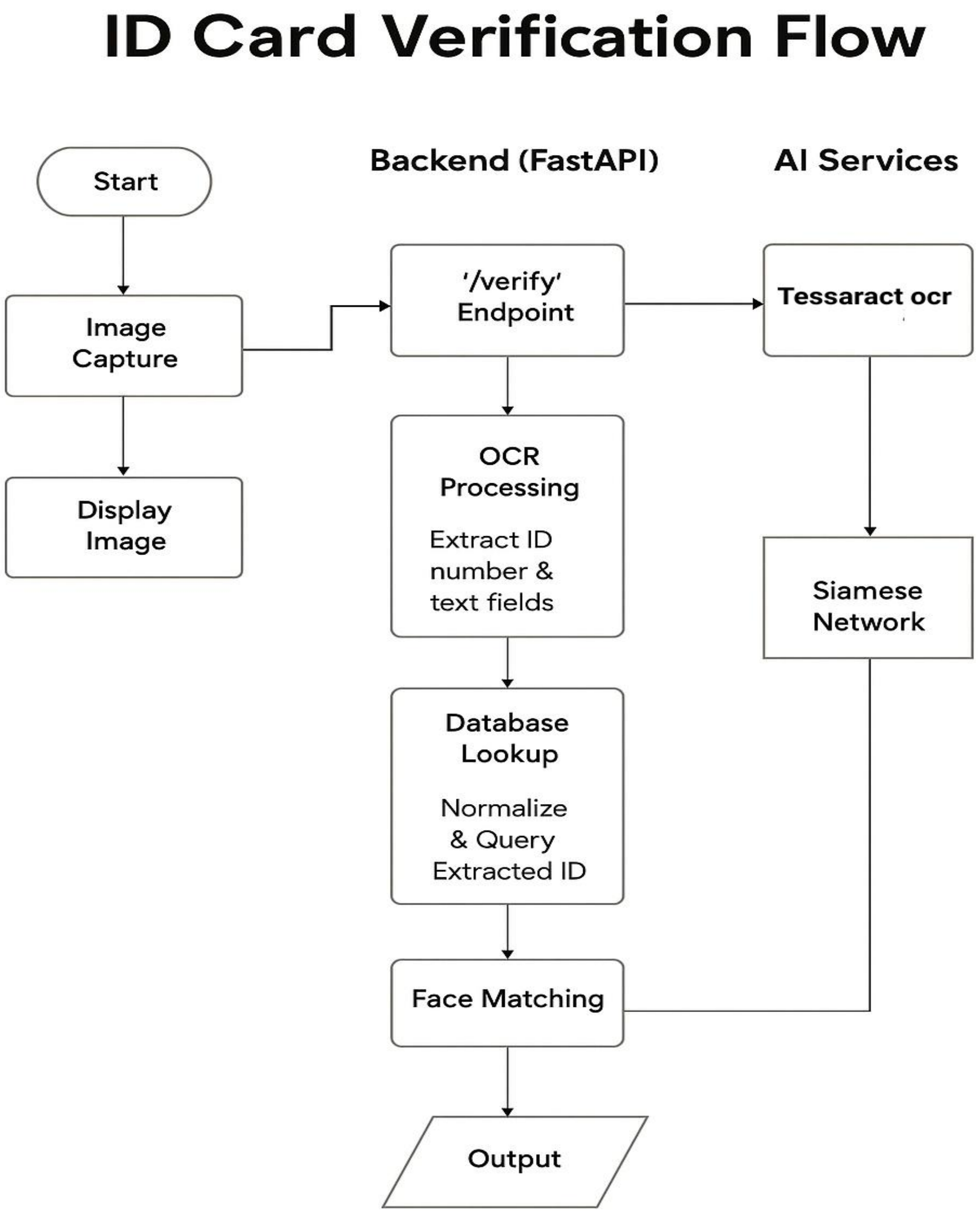


Fig 5.1 Proposed system

1. **Start**

The process begins when the user initiates the ID verification operation, such as uploading or capturing an image of an ID card.

2. **Image Capture**

The system captures the ID card image using a camera or accepts an uploaded image file. This image serves as the input for subsequent verification steps.

3. **Display Image**

The captured image is displayed to the user for confirmation or correction before further processing.

4. **'/verify' Endpoint (Backend – FastAPI)**

Once the image is confirmed, it is sent to the FastAPI backend through the /verify endpoint. This endpoint handles all the communication between the user interface, OCR system, database, and AI services.

5. OCR Processing

In this stage, the backend performs Optical Character Recognition (OCR) to extract key textual information from the ID card image.

The extracted data typically includes:

- ID number
- Name
- Date of birth
- Address or other relevant fields

6. **Tesseract OCR (AI Service)**

The OCR processing uses Tesseract, an open-source OCR engine, to recognize and extract textual information from the ID image.

This service converts the image content into structured text data.

7. **Database Lookup**

The extracted ID number and text fields are normalized (cleaned and standardized) before being queried against the database.

This lookup helps verify if the extracted ID data already exists or matches a registered record.

8. **Siamese Network (AI Service)**

Parallel to text extraction, the Siamese Neural Network model is employed for face matching. It compares the facial image from the ID card with a stored or live-captured image to confirm that both belong to the same person.

The Siamese Network excels in one-shot learning and similarity comparison, making it suitable for identity verification.

9. **Face Matching**

The backend combines the OCR results (ID and textual verification) with the Siamese Network's output (facial similarity score).

If both the text and facial data match within acceptable confidence thresholds, the ID is considered verified.

10. **Output**

Finally, the system produces the verification result, which may include:

- Verification status (Verified / Not Verified)
- Extracted ID details
- Confidence scores from OCR and face matching

The result is then returned to the frontend for display or further action.

Sequence Diagram:

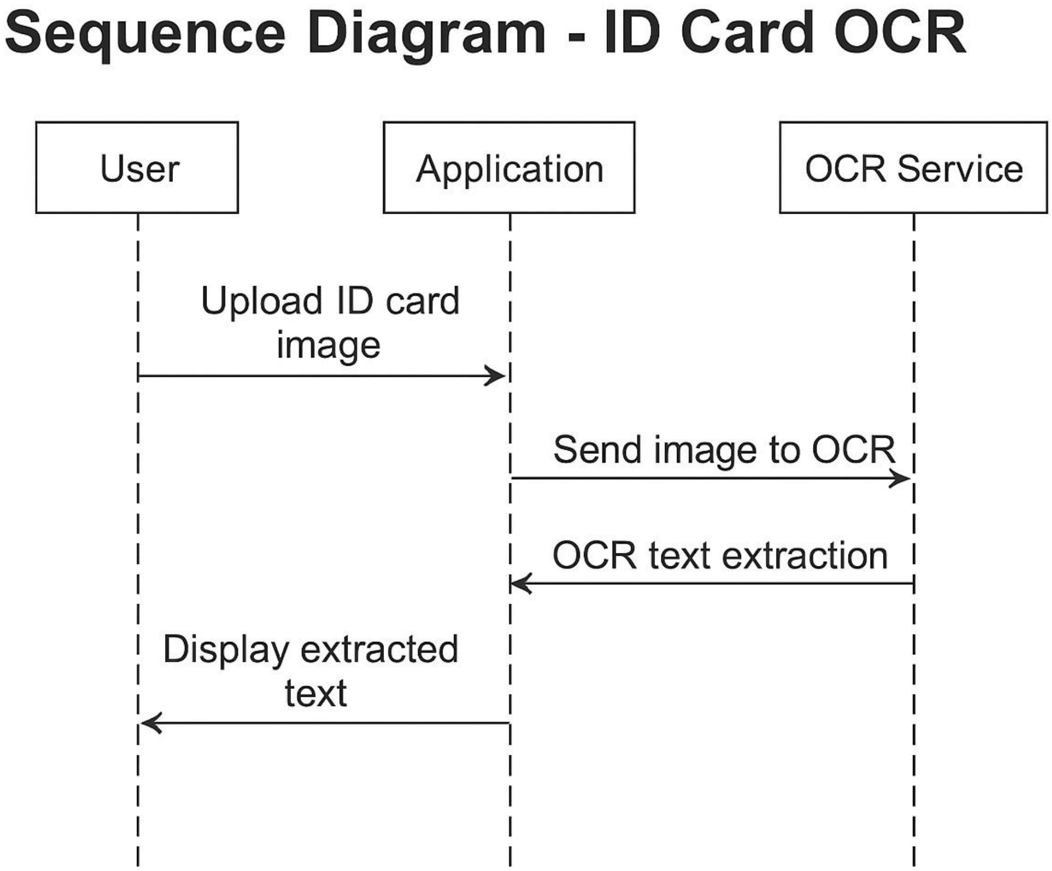


Fig 5.2 Sequence Diagram

1. **User**

The process begins with the User, who initiates the operation by uploading an image of an ID card. This image acts as the input for the OCR pipeline.

2. **Application**

Once the user uploads the image:

- The Application receives the ID card image.
- It then sends the image to the OCR Service for text extraction.
- After receiving the extracted text from the OCR Service, the application processes the output (if

required) and prepares it for display to the user.

3. **OCR Service**

The OCR Service (such as Tesseract or any AI-based OCR engine) is responsible for performing the Optical Character Recognition task:

- It receives the ID card image from the application.
- The OCR engine analyzes the image and extracts text fields such as the name, ID number, date of birth, and other relevant details.
- The recognized text data is then sent back to the Application.

4. **Display Extracted Text**

After receiving the processed text from the OCR Service:

- The Application displays the extracted information to the User.
- This allows the user to view, verify, or edit the recognized text.

Chapter – 6

Experimental Setup

1. Introduction

The experimental setup for the proposed system, **ScanPoint**, was designed to test and evaluate the performance of real-time ID detection and verification. The setup involves both **hardware and software components**, ensuring accurate data acquisition, processing, and output generation. The environment was configured to replicate real-world ID verification conditions such as at college gates, office receptions, and secure zones.

2. Hardware Requirements :

Component	**Specification / Purpose**
Camera / Webcam	1080p HD resolution camera for capturing ID card and live face.
Processor	Intel i5 or higher for efficient real-time computation.
RAM	Minimum 8 GB for smooth processing of images and OCR tasks.
Storage	256 GB SSD for faster data access and retrieval.
Lighting Setup	Uniform lighting to avoid reflection and shadows on ID cards.
Network	Internet/Wi-Fi for database connectivity and cloud verification.

3. Software Requirements :

Component	**Tool / Framework**
Operating System	Windows 10 / Ubuntu 22.04
Programming Language	Python 3.9
Libraries Used	OpenCV (for image capture and preprocessing), Tesseract OCR (for text extraction), Face Recognition (for identity matching), NumPy, Pandas
Database	MySQL / Firebase (for storing authorized IDs and verification logs)
IDE / Platform	Jupyter Notebook / VS Code
Frontend (Optional)	Flask or Streamlit (for GUI and web interface)

4. System Configuration and Environment :

- The camera was mounted at a fixed angle on a stand for consistent ID capture.
- The system was tested under normal indoor lighting and controlled background.
- IDs of students/employees were stored in the database prior to testing.
- Each ID verification test included:
  - Image capture
  - Preprocessing (resizing, denoising, and thresholding)
  - OCR and face recognition
  - Database validation
  - Display of result

5. Experimental Procedure :

1. **Initialization:** The system initializes the camera and connects to the database.
2. **ID Capture:** The user places their ID card in front of the camera.
3. **Preprocessing:** The captured frame undergoes brightness adjustment and cropping.
4. **Text Extraction:** OCR extracts ID details (Name, ID Number, Department, etc.).
5. **Face Matching:** Real-time image of the user is captured and compared with the ID photo.
6. **Verification:** The extracted details are matched with the database records.
7. **Result Output:** The system displays “Verified” or “Not Verified” on the interface.

6. Experimental Results and Observations :

- Average ID detection and OCR time: **1.8 seconds**
- Average face verification time: **2.3 seconds**
- Overall accuracy: **≈ 95%** under good lighting conditions
- Performance drops slightly in low light or blurred ID images

7. Conclusion :

The experimental setup demonstrates that **ScanPoint** efficiently performs real-time ID verification using OCR and facial recognition. The setup can be easily deployed in institutions or organizations to enhance access security and reduce manual verification efforts.

Chapter 7

Project Planning

July

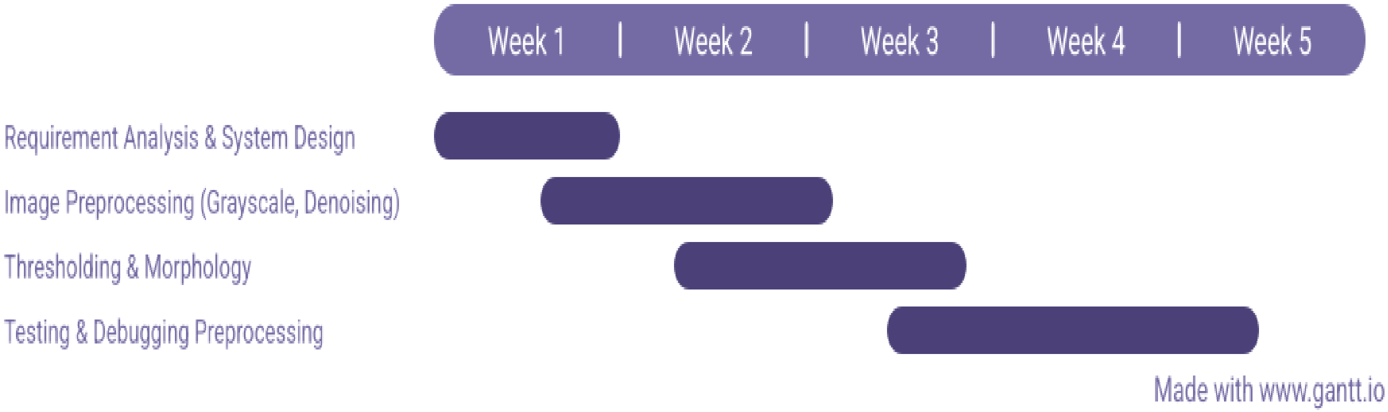


Fig 7.1 July (Gantt Chart)

August

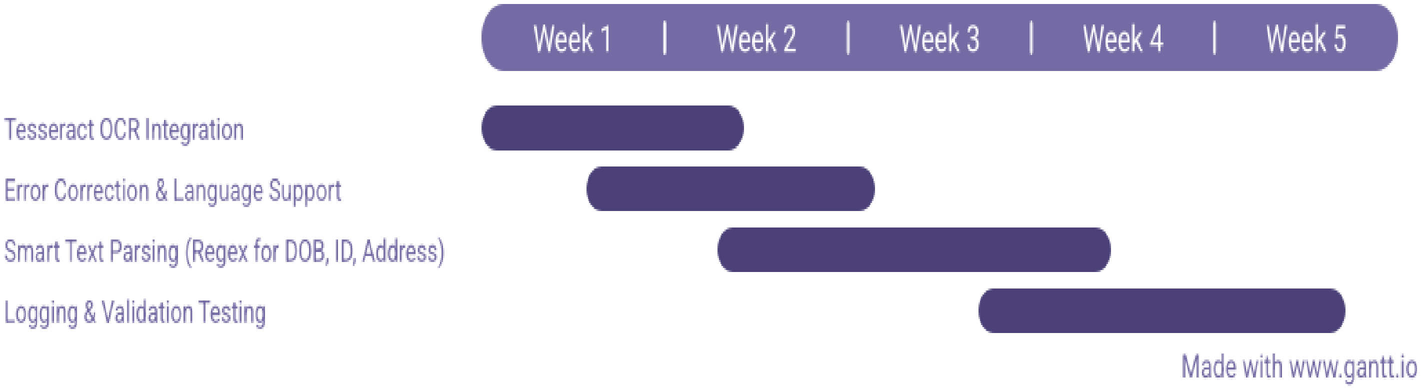


Fig 7.2 August (Gantt Chart)

September

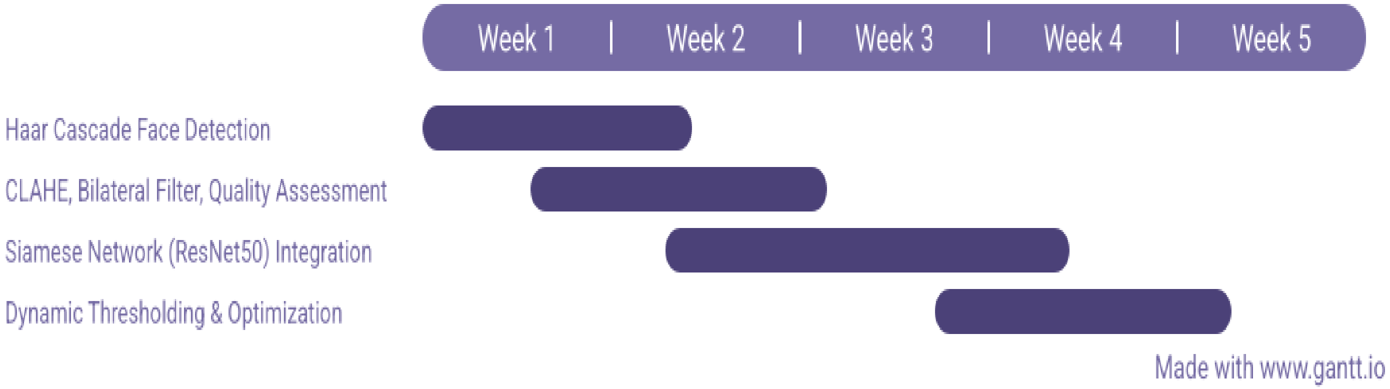


Fig 7.3 September (Gantt Chart)

October

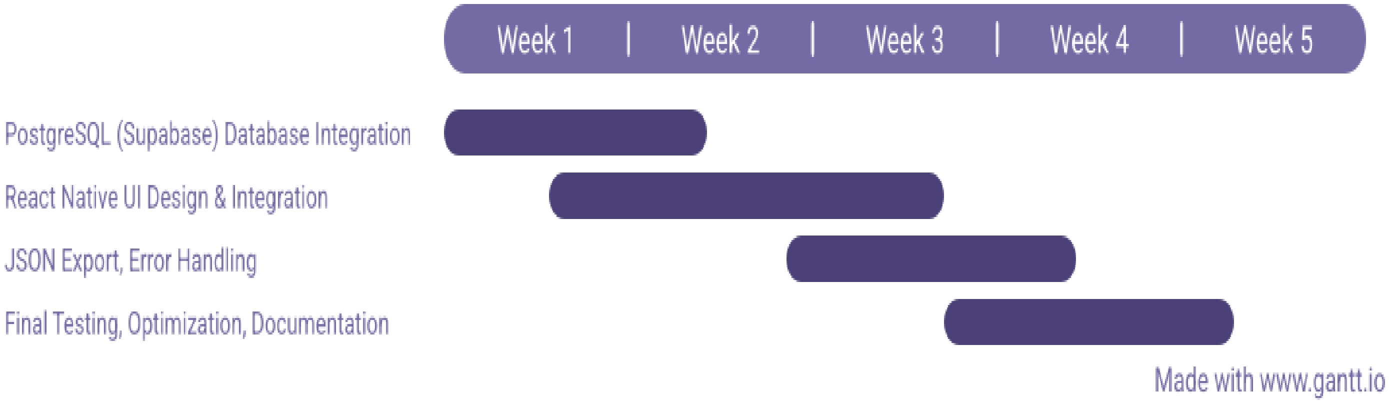
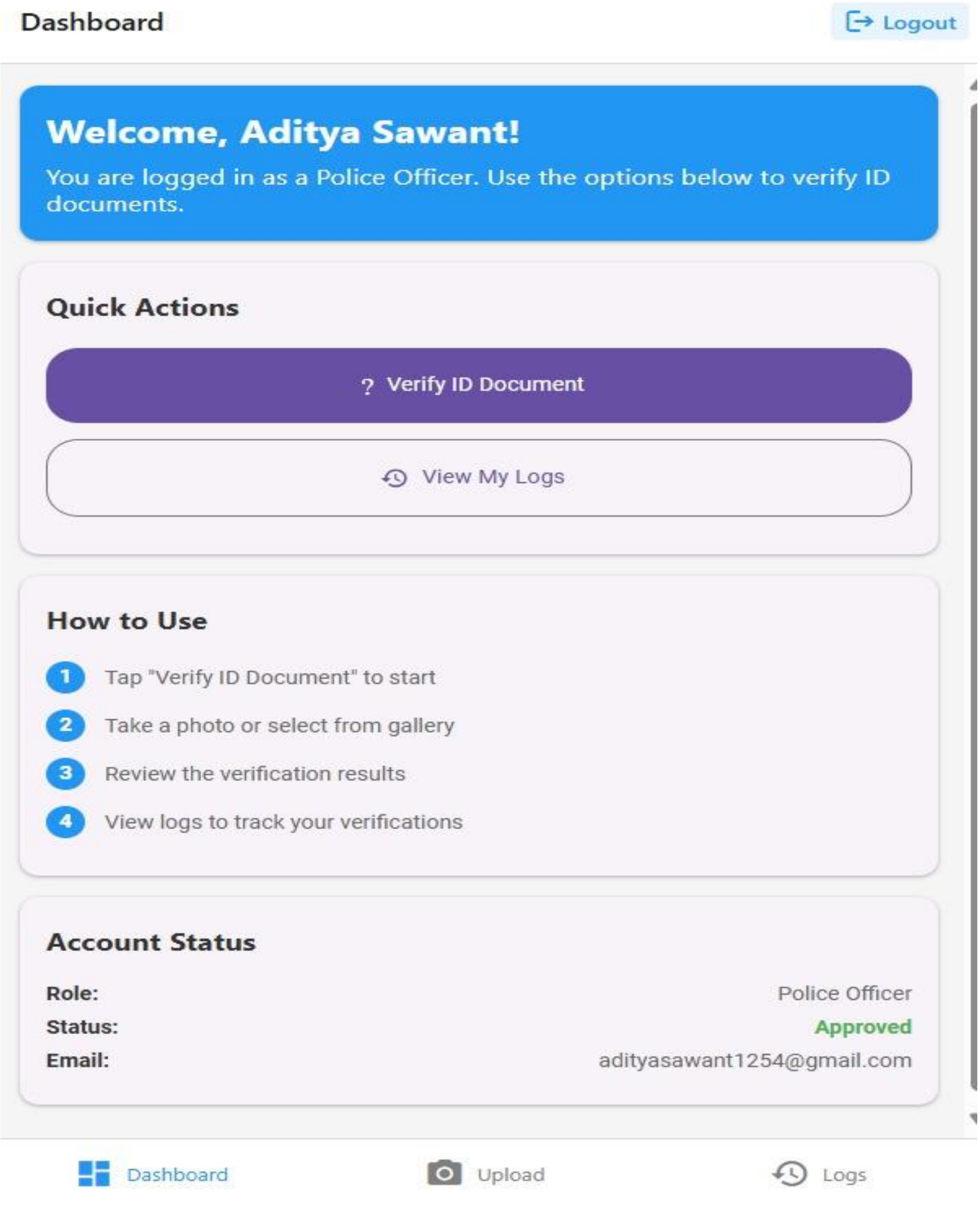


Fig 7.4 October (Gantt Chart)

Chapter – 8

Expected Output



Welcome, Aditya Sawant!

You are logged in as a Police Officer. Use the options below to verify ID documents.

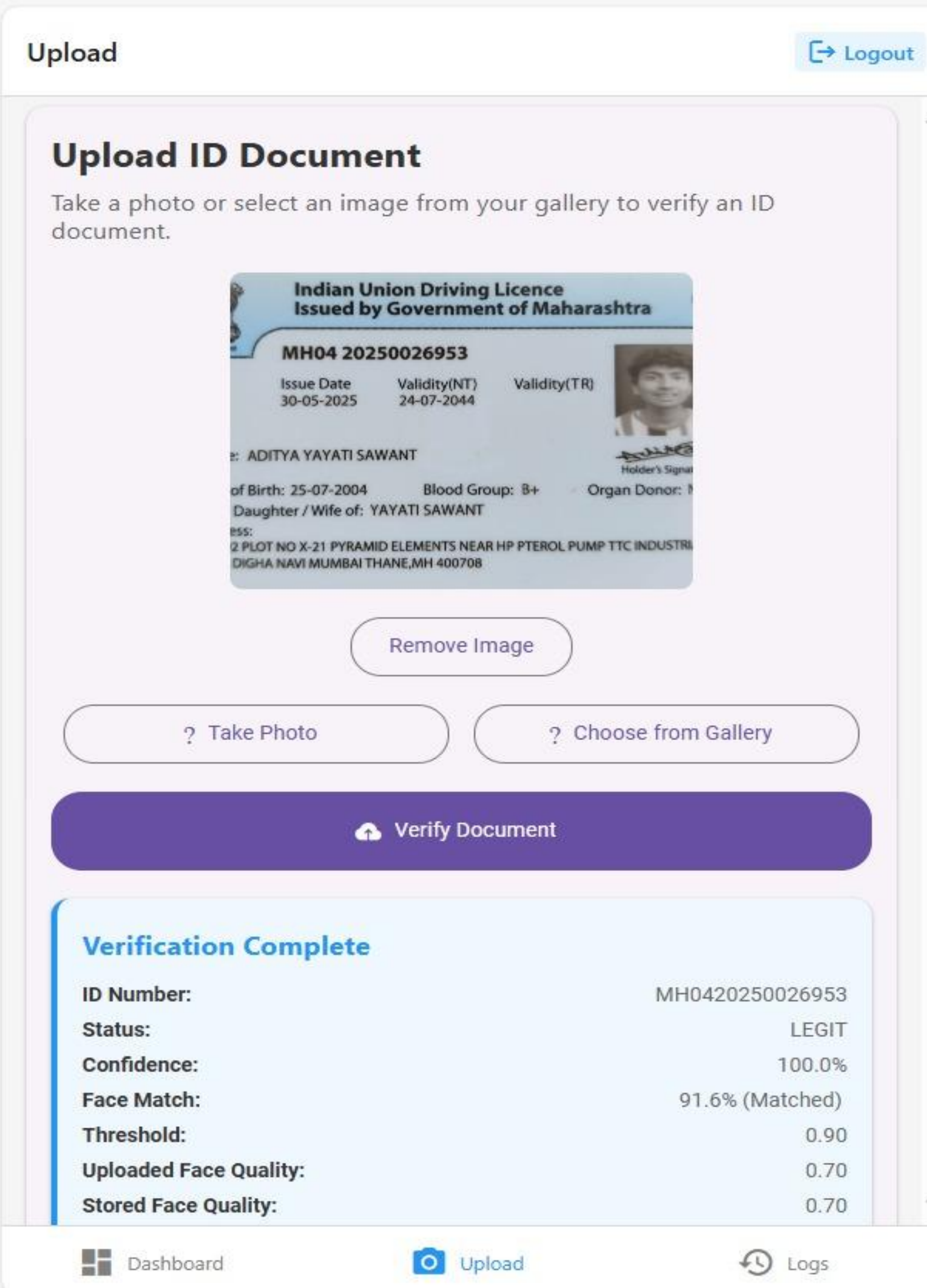
How to Use

1. Tap "Verify ID Document" to start
2. Take a photo or select from gallery
3. Review the verification results
4. View logs to track your verifications

Account Status

Role:	Police Officer
Status:	Approved
Email:	adityasawant1254@gmail.com

Fig 8.1 User Interface



Upload ID Document

Take a photo or select an image from your gallery to verify an ID document.

Indian Union Driving Licence
Issued by Government of Maharashtra

MH04 20250026953

Issue Date 30-05-2025 Validity(NT) 24-07-2044 Validity(TR)

e: ADITYA YAYATI SAWANT

Holder's Signa

of Birth: 25-07-2004 Blood Group: B+ Organ Donor: N

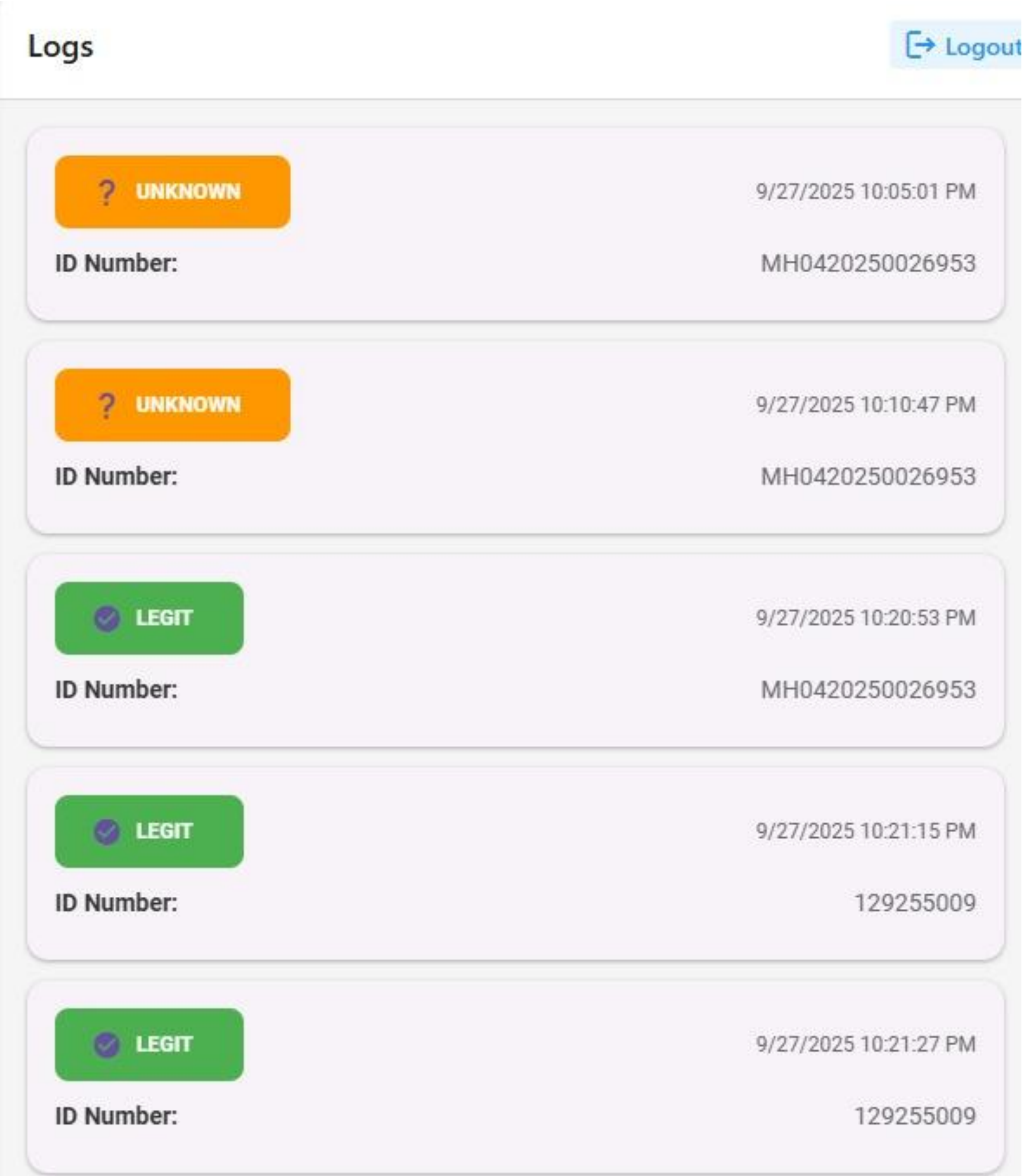
Daughter / Wife of: YAYATI SAWANT

ess:
2 PLOT NO X-21 PYRAMID ELEMENTS NEAR HP PTEROL PUMP TTC INDUSTRI
DIGHA NAVI MUMBAI THANE,MH 400708

Verification Complete

ID Number:	MH0420250026953
Status:	LEGIT
Confidence:	100.0%
Face Match:	91.6% (Matched)
Threshold:	0.90
Uploaded Face Quality:	0.70
Stored Face Quality:	0.70

Fig 8.2 ID Card Upload and Verification Process



Logs

? UNKNOWN 9/27/2025 10:05:01 PM

ID Number: MH0420250026953

? UNKNOWN 9/27/2025 10:10:47 PM

ID Number: MH0420250026953

✓ LEGIT 9/27/2025 10:20:53 PM

ID Number: MH0420250026953

✓ LEGIT 9/27/2025 10:21:15 PM

ID Number: 129255009

✓ LEGIT 9/27/2025 10:21:27 PM

ID Number: 129255009

Fig 8.3 System Log Interface Displaying ID Verification Status and History

REFERENCES

[1] S. Kilany, R. Al-Hadad, F. Al-Hadad and H. Ahmed, “A Comprehensive Survey of Deep Face Verification Systems,” Scientific Reports (Nature), vol. 15, art. 15753, Jan. 2025. [Online]. https://www.nature.com/articles/s41598-025-15753-8

[2] M. Arif, R. Kumar, A. Sheikh and N. Kumar, “Siamese Networks for Multiple Face-Detection and Identification,” Proceedings of the International Conference on Next Generation Information System Engineering (NGISE), Mar. 2025. [Online].
(https://www.researchgate.net/publication/394585881_Siamese_Networks_for_Multiple_Face-Detection_and_Identification

[3] D. Bhattacharya, A. Gajool, S. Banage, S. Bhute and D. V. Gore, “Face Verification using Twin Convolutional Neural Networks,” Conference Paper, PES Modern College of Engineering, Jun. 2025. [Online].
https://www.researchgate.net/publication/392405618_Face_Verification_using_Twin_Convolutional_Neural_Networks

[4] A.J. Jayachandran, “Investigating Fairness in Facial Verification with Siamese Neural Networks,” ACM Proceedings, Oct. 2024. [Online].
https://dl.acm.org/doi/10.1145/3701268.3701276

[5] S. Carta, “An End-to-End OCR-Free Solution For Identity Document Recognition (IDR),” Procedia Computer Science (Elsevier), vol. 232

[6] S. Dhakal, S. Sigdel, S. P. Paudel, S. K. Ranabhat and N. Lamichhane, “Mero Nagarikta: Advanced Nepali Citizenship Data Extractor with Deep Learning-Powered Text Detection and OCR,” *arXiv preprint arXiv:2410.05721*, Oct. 2024. [Online].
https://arxiv.org/abs/2410.05721

[7] J. Lerouge, G. Betmont, T. Bres, E. Stepankevich and A. Bergès, "DocXPand-25k: A Large and Diverse Benchmark Dataset for Identity Documents Analysis," *arXiv preprint arXiv:2407.20662*, Jul. 2024. [Online]. https://arxiv.org/abs/2407.20662

[8] A. M, D. S, S. N, T. Thishavarthani and D. Deva, "AI Powered Image Processing System for Automated Aadhaar and Smart Card Verification," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 13, no. 6, June 2025. [Online].
https://www.ijcrt.org/papers/IJCRT2506691.pdf

[9] V. Kumar, "Siamese-based Offline Word Level Writer Identification in a Residual Framework," *Pattern Recognition Letters*, vol. 180, pp. 34-42, 2024. [Online]. Available: (search article by title) — Note: uses Siamese network in document/hand-writing domain.

[10] "Identity document (ID) OCR | Automate ID processing with AI," ABBYY Documentation, Apr. 2024. [Online].
https://www.abbyy.com/marketplace/assets/host/abbyy/document-skill/identity-documents-id/ ABBYY