Optimized Hybrid KYC Verification System

CAPSTONE PROJECT REPORT

Submitted to

by

NEHA BARTHAKUR

SUMMARY

The bank's digital KYC (Know Your Customer) process, while innovative, has been plagued by high rejection rates and customer abandonments, leading to suboptimal conversion rates and increased operational costs. Key issues include user errors during document selection and scanning, network-related upload failures, server-side validation delays, and mismatches in identity verification. This report evaluates a comprehensive solution that integrates client-side enhancements (such as on-device AI for auto-detection and quality checks) with server-side optimisations (like improved OCR, asynchronous processing, and human-in-loop reviews) to address these pain points.

The proposed solution directly targets all identified failure stages, aiming to reduce overall rejections by 50-70%. It emphasises fewer abandonments through intuitive UX, faster turnaround times (TAT) via automation and pre-checks, clearer next-step visibility with structured error messaging, and fewer re-submissions by providing guided retries and escalations. Expected outcomes include failure rate reductions across stages: from 15% to 3-5% in document selection, 35% to 10-15% in scanning, and similar improvements elsewhere.
While the solution is robust, residual risks such as device compatibility and network variability must be mitigated through fallbacks and monitoring. This report outlines detailed mappings, metrics, implementation steps, and monitoring strategies to ensure measurable success. Implementation should begin with an MVP focused on auto-detection and client pre-checks, followed by A/B testing and dashboard instrumentation.

By adopting this approach, the bank can achieve a more seamless, user-friendly KYC experience, aligning with regulatory requirements (e.g., mandatory PAN and Aadhaar for digital accounts) and boosting customer satisfaction and retention.

1. Problem Statement

The bank's digital KYC system enables customers to onboard via the mobile app by selecting, scanning, and uploading identity documents (e.g., Aadhaar Card, PAN Card, Voter ID, Passport) along with photographs for verification. However, since its launch, the system has experienced elevated rejection rates, contributing to high customer drop-offs and lost business opportunities. Customers are limited to three attempts per stage, with a fourth attempt resulting in automatic rejection.

Key failure stages and their percentages, as provided:

- Select Document Type: 15% failure rate, often due to user confusion or incorrect selections.
- Scan Document: 35% failure rate, primarily from improper scanning (e.g., blur, glare, wrong orientation).
- Upload Document: 25% failure rate, linked to network issues, file size problems, and server timeouts.
- KYC Check: 15% failure rate, caused by OCR inaccuracies, duplicates, or validation errors.
- KYC Approval: 10% failure rate, stemming from face mismatches, liveness failures, or non-compliance with guidelines (e.g., passport validity, photo matching).

Known root causes include duplicate documents in the database, server response times exceeding 15-20 seconds, and scanning quality issues. These lead to broader challenges: high abandonments (customers leaving mid-process), prolonged TAT (turnaround time), unclear guidance on next steps, and frequent re-submissions.

Regulatory guidelines further complicate the process:

- Acceptable documents: Aadhaar, Passport, Voter ID for address proof; PAN, Aadhaar, Passport for identity proof.
- Mandatory: PAN and Aadhaar for digital accounts.
- Additional requirements: Passport-size photo upload, real-time photo for verification, minimum 6-month passport validity, and photo matching.
- Attempt limits: Three per stage.

The goal is to redesign the process for:

- Fewer abandonments: By simplifying user interactions and reducing friction.
- Faster TAT: Targeting sub-20-second responses per step.
- Clearer next-step visibility: Providing specific error messages and guidance.
- Fewer re-submissions: Through proactive quality checks and automated corrections.

2. Objectives

This report reconstructs and expands upon the proposed solution, mapping features to failure stages, estimating improvements, identifying risks, defining metrics, and outlining an implementation roadmap. It aims to provide a actionable, lengthy blueprint for stakeholders to deploy and monitor enhancements.

3. Proposed Solution Overview

The solution adopts a hybrid approach: leveraging on-device AI (e.g., machine learning models for document classification and image processing) to handle client-side issues in real-time, while optimising server-side workflows for efficiency and accuracy. This includes:

- Client-Side Improvements: Auto-detection of document types, quality heuristics for scans, pre-upload checks, and intuitive UX overlays.
- Server-Side Enhancements: Advanced OCR with MRZ/QR parsing, robust duplicate detection, asynchronous processing, and human escalation for ambiguous cases.
- UX and Process Changes: Structured error codes, progress indicators, attempt counters, and clear messaging to guide users.

This holistic strategy ensures compliance with KYC guidelines while minimizing user effort. For instance, auto-detection eliminates the dropdown menu, reducing selection errors, and on-device checks prevent uploads of low-quality scans, cutting down on server rejections.

The solution is feasible with existing technologies (e.g., TensorFlow Lite for on-device ML, cloud-based OCR APIs like Google Vision or AWS Rekognition) and can be rolled out iteratively to minimize disruption.

4. Features Addressing Each Failure Stage

To ensure comprehensive coverage, the solution maps specific features to each failure stage. This section details how each feature mitigates primary causes, with explanations of mechanisms and benefits.

1. Select Document Type (15% Failure Rate)

Primary Causes: User confusion in dropdown selection, leading to mismatches or invalid choices.

Solution Features:

- On-device document classifier: Uses AI to automatically detect document type (e.g., Aadhaar vs. PAN) via camera preview.
- Auto-detect and confirmation: Displays detected type with a UX overlay (e.g., "Detected: Aadhaar Card – Confirm?") to eliminate manual selection.
- Auto-capture integration: Seamlessly transitions to scanning once confirmed.

This removes human error from the equation, ensuring only valid, guideline-compliant documents (e.g., mandatory PAN/Aadhaar) proceed. This reduces abandonments by making the process feel effortless. It also upports multi-document uploads (e.g., PAN + Aadhaar) with smart sequencing.

2. Scan Document (35% Failure Rate)

Primary Causes: Poor image quality (blur, glare, improper framing, wrong side scanned), bad lighting, or user inexperience.
Solution Features:

- Auto-crop and perspective correction: AI adjusts for angles and crops to focus on the document.
- Auto-capture trigger: Captures image automatically when alignment, focus, and lighting are optimal.
- Image quality heuristics: Real-time checks for blur, glare, corners detection; rejects subpar scans before upload.
- Contextual hints: On-screen guidance like "Hold steady," "Move to better light," or "Flip to front side."

This prevents low-quality submissions at the source, reducing re-submissions and TAT. For example, if glare is detected, the app prompts the user to adjust positioning immediately.It also integrates with device hardware (e.g., flashlight toggle) for low-light scenarios, ensuring higher success on first attempts.

3. Upload Document (25% Failure Rate)

Primary Causes: Network instability, large file sizes, server timeouts, or repeated failures exhausting attempts.
Solution Features:

- Client-side pre-checks: Compress/resize images, validate file integrity before upload.
- Idempotent uploads: Allows retries without duplicating data; uses unique IDs to resume interrupted uploads.
- Progress UI and circuit-breakers: Shows real-time upload status; switches to offline queueing if network is poor.

- Async queueing and human fallback: Background uploads with notifications; escalates to support if failures persist.

It minimizes drop-offs from technical glitches by handling errors gracefully, ensuring TAT stays under 20 seconds even in suboptimal conditions. It also reduces server load by filtering invalid uploads, indirectly improving overall system responsiveness.

4. KYC Check (15% Failure Rate)

Primary Causes: OCR failures on text extraction, duplicate detections, or business rule violations (e.g., expired passport).
Solution Features:

- High-quality server OCR with MRZ/QR parsing: Extracts data from machine-readable zones for accuracy.
- Robust duplicate detection: Uses fuzzy matching and biometric hashes (with consent) to avoid false positives.
- Structured error codes: Returns specific reasons (e.g., "Duplicate Aadhaar detected") for client-side display.
- Human-in-loop review: Flags ambiguous cases for quick manual verification.

It enhances validation precision, reducing unnecessary rejections and providing clear next steps (e.g., "Upload alternate document"). And complies with guidelines by auto-checking validity (e.g., passport >6 months).

5. KYC Approval (10% Failure Rate)
Primary Causes: Face/photo mismatches, liveness detection failures, missing mandatory docs, or non-matching real-time photos.
Solution Features:

- Face-match and liveness detection: AI compares uploaded photo with real-time capture, ensuring authenticity.
- On-capture checks: Validates passport expiry and mandatory docs (PAN + Aadhaar) during upload.
- Clear messaging and escalation: Displays "Photo mismatch – Retake?" with attempt counters; routes to support on near-failure.

It streamlines final verification, reducing abandonments by guiding users through corrections before rejection and improves security while maintaining user trust through transparent processes.

5. Expected Outcomes and Improvement Targets

Implementing the solution should yield significant reductions in failure rates, leading to the desired outcomes. These targets are based on industry benchmarks (e.g., similar fintech apps achieving < 5% per-stage failures) and conservative estimates, assuming phased rollout and tuning.

- Select Document Type: Reduce from 15% to 3-5%. Auto-detection virtually eliminates manual errors, fostering fewer abandonments and clearer visibility.
- Scan Document: Reduce from 35% to 10-15%. Quality heuristics and auto-capture minimize re-submissions, speeding TAT.
- Upload Document: Reduce from 25% to 8-12%. Pre-checks and async handling address network issues, reducing drop-offs.
- KYC Check: Reduce from 15% to 6-8%. Advanced parsing and reviews improve accuracy, enhancing next-step guidance.
- KYC Approval: Reduce from 10% to 3-5%. Robust matching ensures faster approvals.

Overall: 50-70% drop in total rejections/abandonments, with TAT <20 seconds per step and +20-40% uplift in conversions. These are measurable KPIs, adjustable based on A/B testing data.

6. Remaining Risks and Edge Cases

Despite the solution's coverage, some risks persist and require mitigations:

- Low-End Devices: On-device AI may lag on older hardware. Mitigation: Provide server-side fallback options and optimize models for efficiency.
- Poor Network Conditions: Uploads could still fail in remote areas. Mitigation: Implement offline queuing and background sync, with user notifications.
- Duplicate Detection False Positives: Overly strict rules might reject valid users. Mitigation: Tune thresholds with real data, incorporate human reviews, and monitor rejection appeals.
- Regulatory/Privacy Constraints: Biometric data handling must comply with laws (e.g., GDPR-like standards in India). Mitigation: Ensure explicit consent, secure storage, and audit trails.
- OCR Blindspots: Rare document variants (e.g., damaged cards) may fail. Mitigation: Retrain models periodically using failure logs and diversify training data.
- User Variability: Elderly or tech-novice users might struggle with auto-features. Mitigation: Offer optional manual modes and in-app tutorials.

Regular audits and user feedback loops will help identify and address these.

7. Visual Representations

To aid stakeholder understanding and facilitate development hand-off, the following diagrams illustrate the end-to-end enhanced digital KYC process.

a. System Architecture

This diagram depicts the layered architecture and data flow between the web client, edge services, and backend systems. Key components include on-device ML modules, compression & idempotent upload mechanisms, CDN/API gateways, advanced OCR/MRZ parsing, duplicate detection, face-match/liveness engines, business rules, and the async/human review queue, and audit logging.

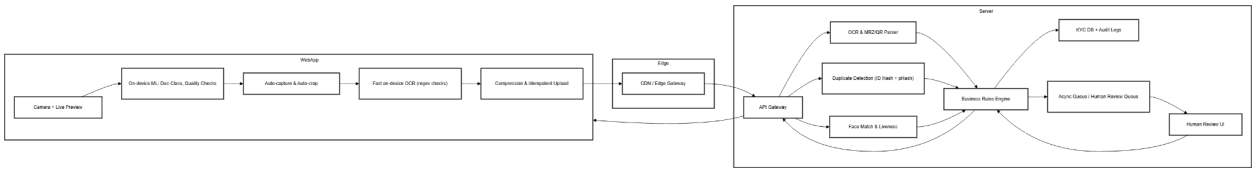

Figure 1: System Architecture

b. Use-Case Diagram

This simplified use-case diagram identifies the primary actors (User and Reviewer) and core use cases: Start KYC Process, Auto-Capture Document (with fallback to Manual Upload), Show Hints/Pre-check, Server Validation, and Human Review Case. Extensions for blur/glare handling and validation errors are clearly marked.

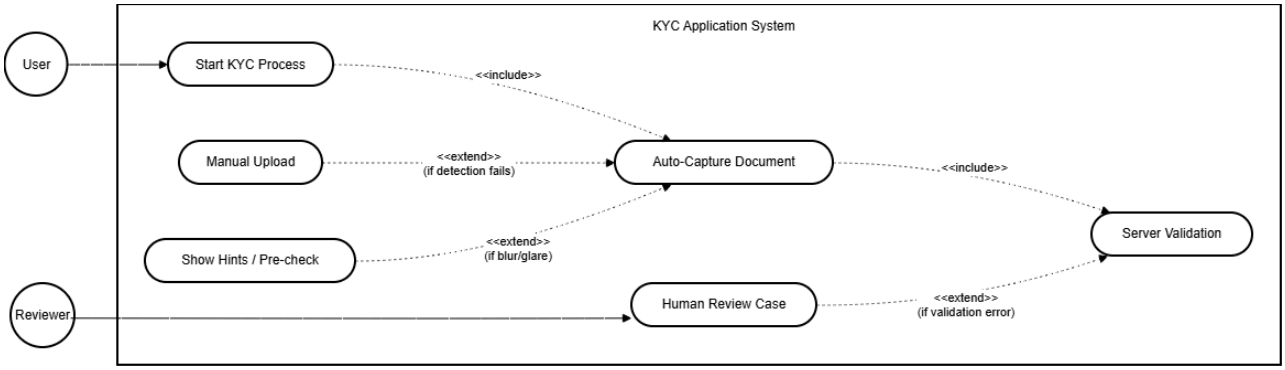

Figure 2: Use-Case Diagram

c. Sequence Diagram

This sequence diagram shows the real-time interaction between User → Web App → OnDeviceML → API → Server → (optional) Human Reviewer. It highlights streaming frames for live detection, auto-capture triggers, pre-checks, compressed upload with metadata, server-side OCR & validation, structured result codes, and the human-in-the-loop escalation path for ambiguous cases.

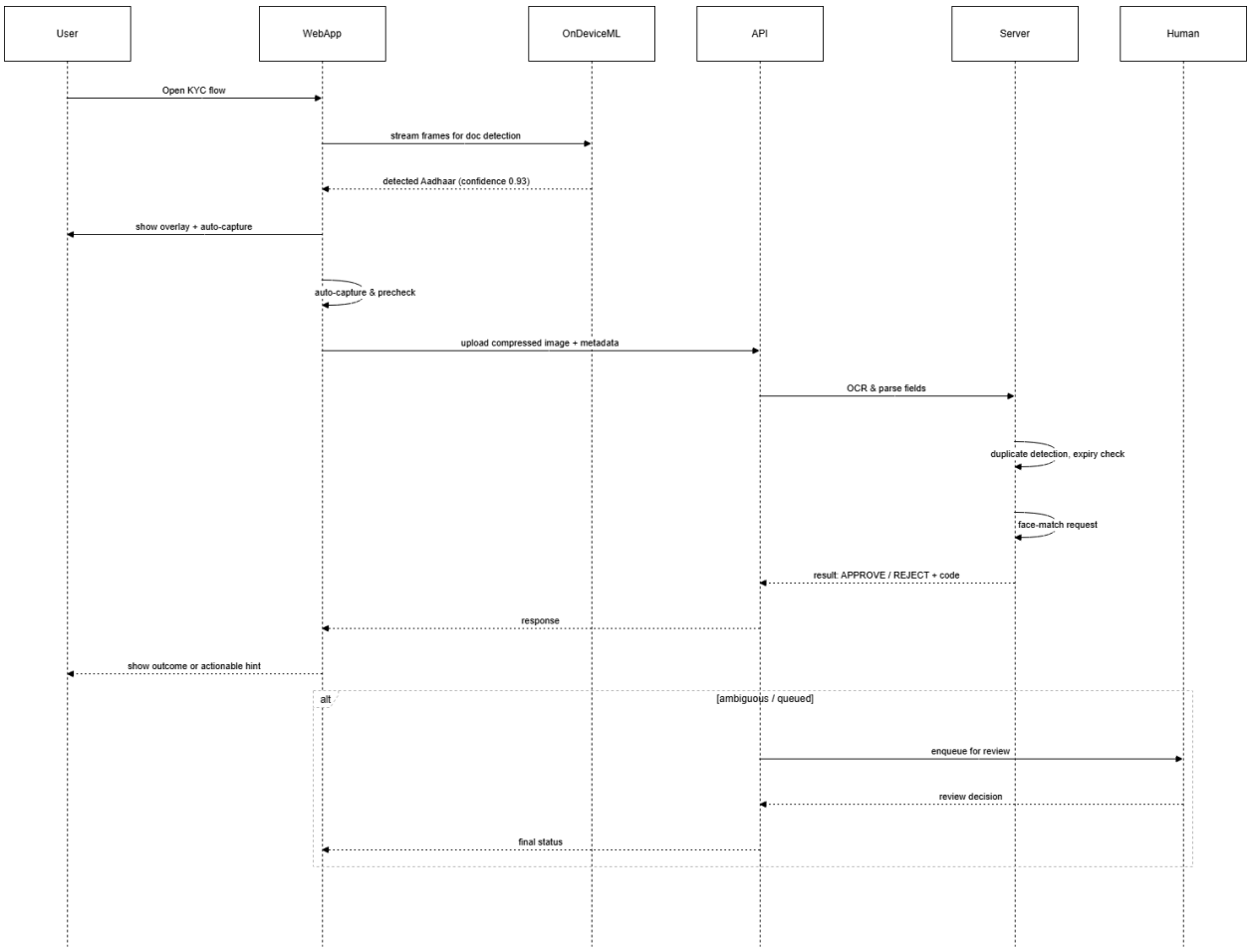

Figure 3: Sequence Diagram

d. Flowchart

This comprehensive flowchart maps the complete user journey from KYC initiation through auto-detection, quality pre-checks, upload, server validation, attempt counting (max 3+1), structured error messaging, guided retries, and final approval or rejection. Decision diamonds and retry loops illustrate how the proposed features dramatically reduce drop-offs and re-submissions.

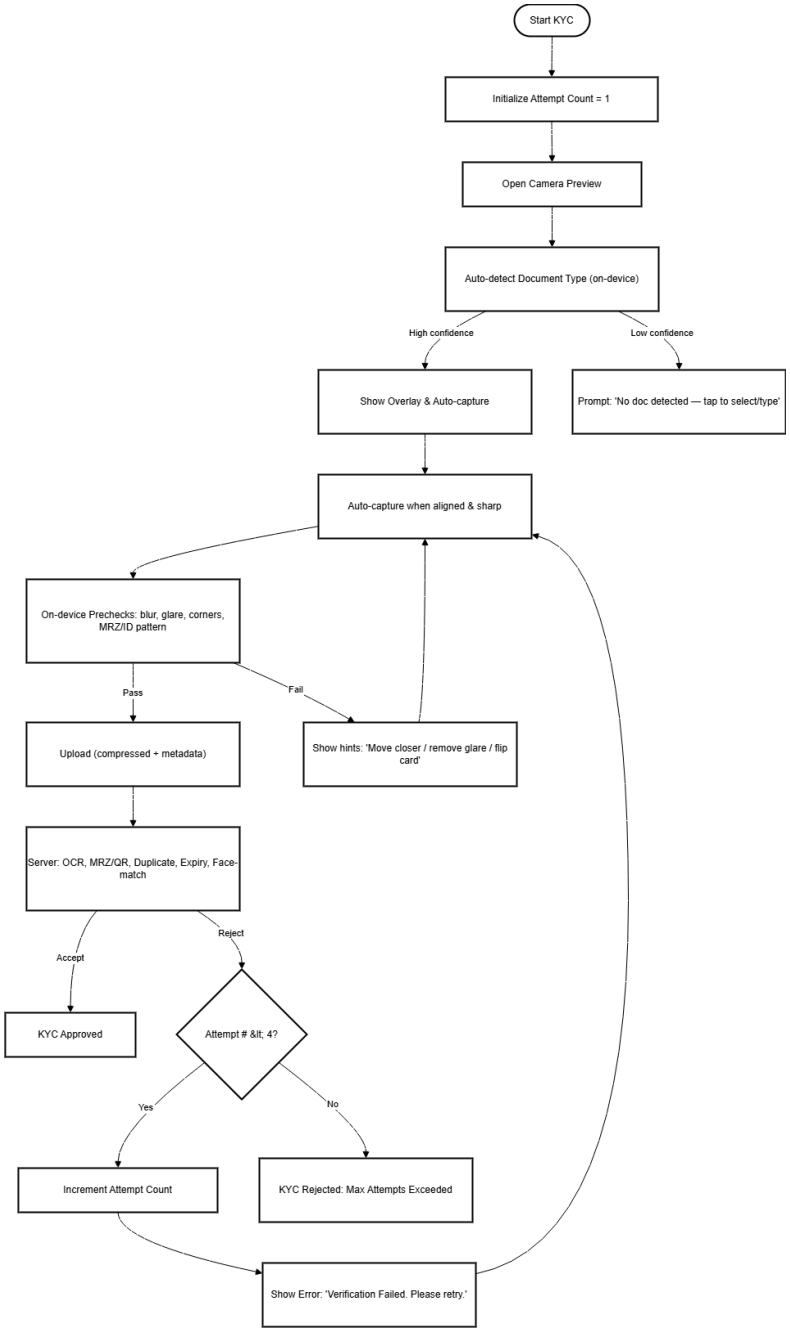

Figure 4: Flowchart

8. Implementation and User Interface Walkthrough

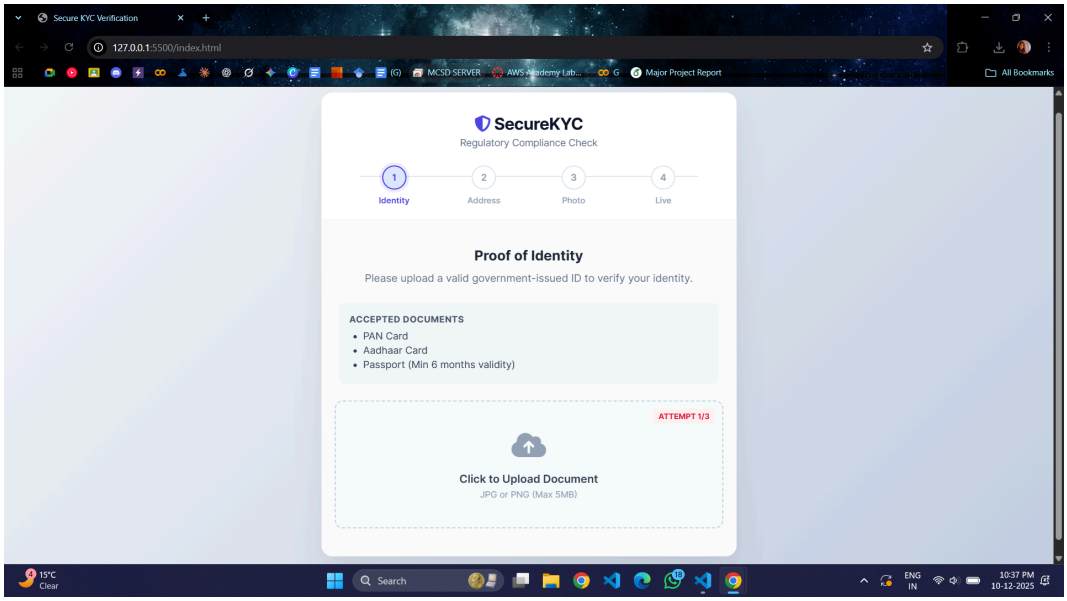

Figure 5: A Simple WebApp

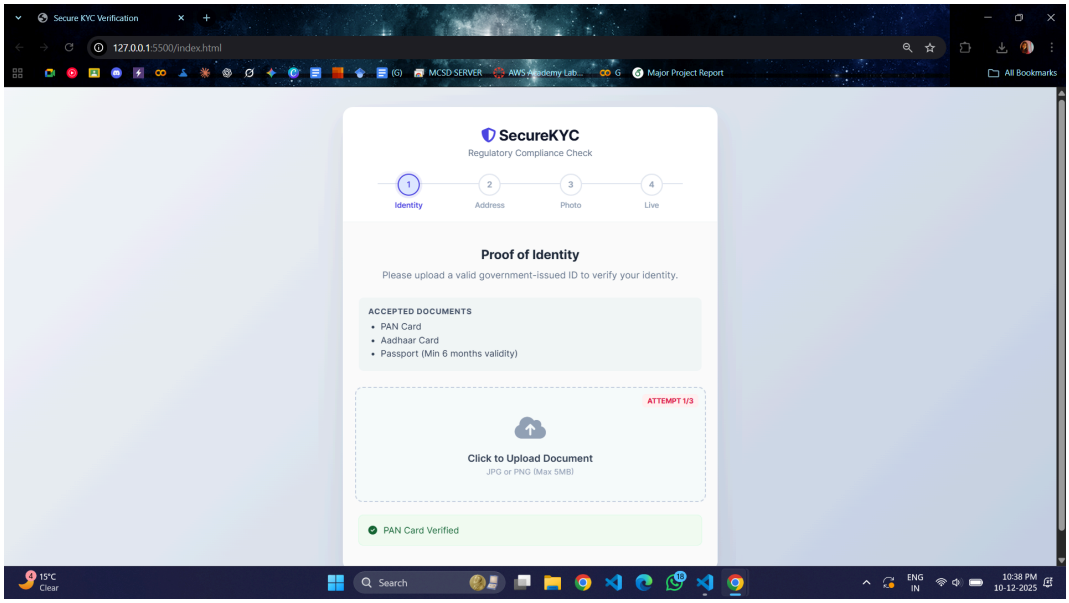

Figure 6: Successful Document Upload

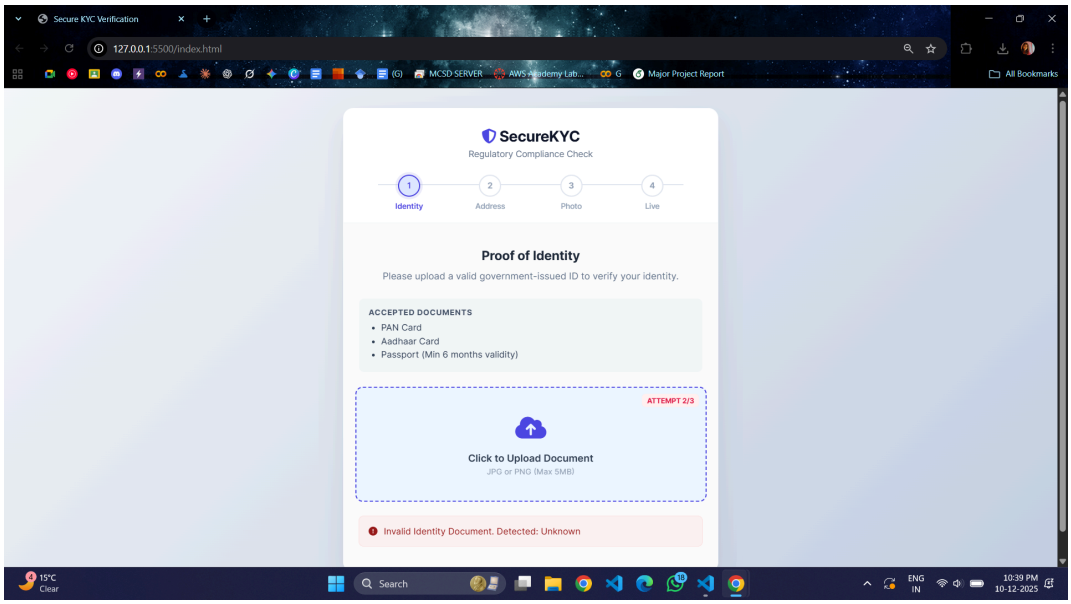

Figure 7: Unsuccessful Attempt

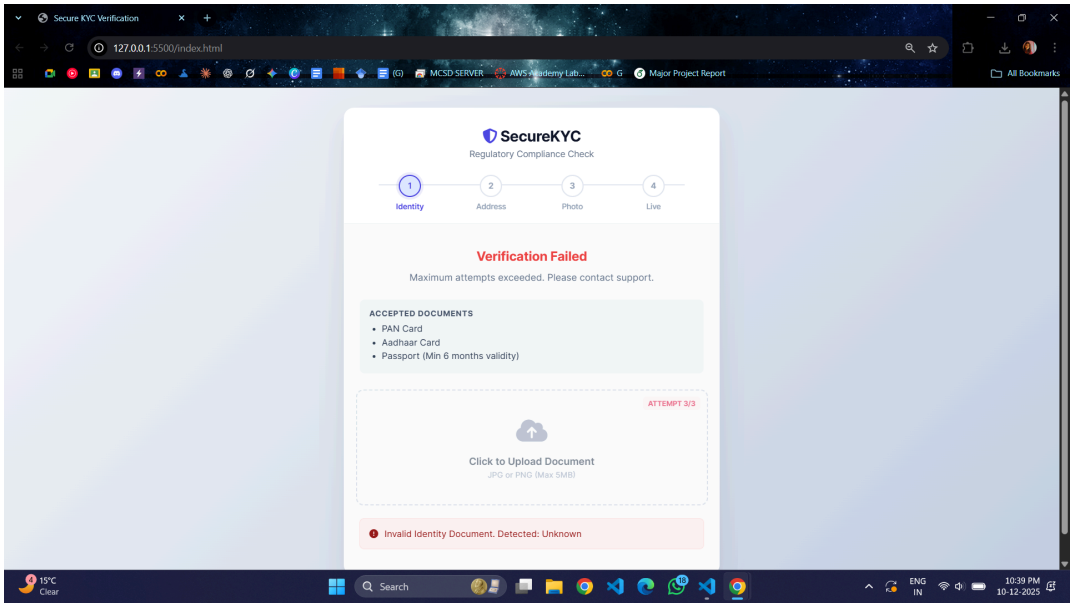

Figure 8: Failure after 3rd Attempt

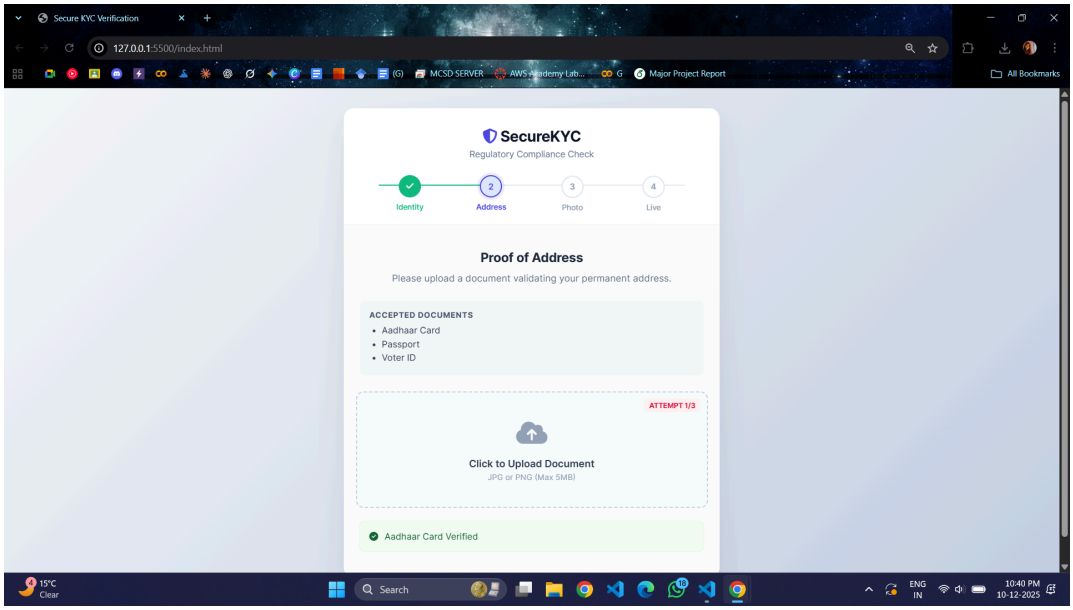

Figure 9: Successful Address Proof Submission

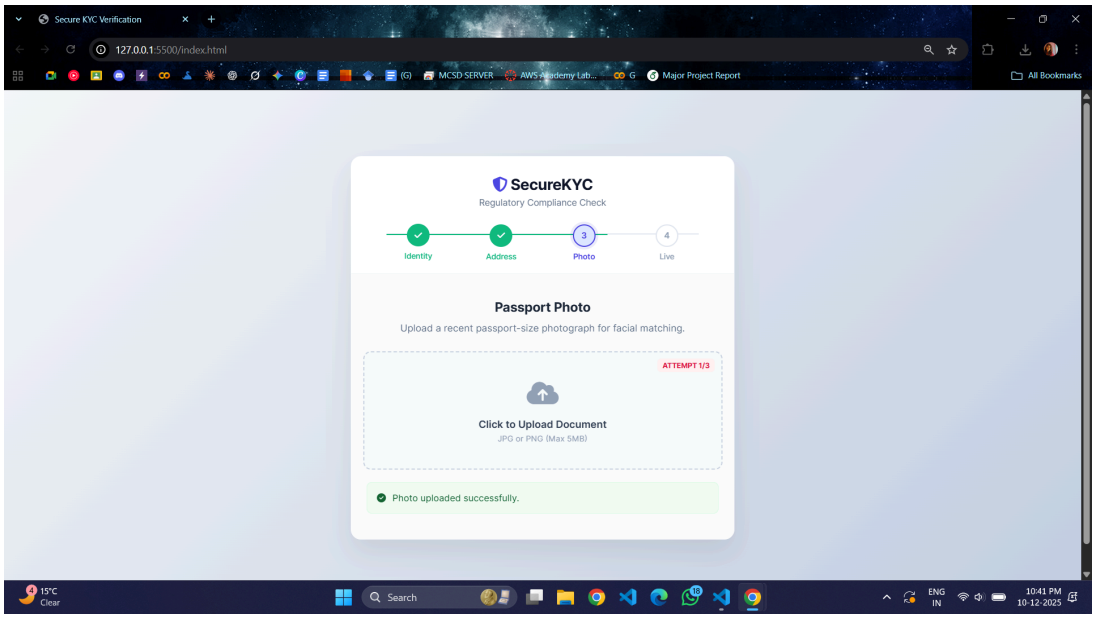

Figure 10: Successful Photo Upload

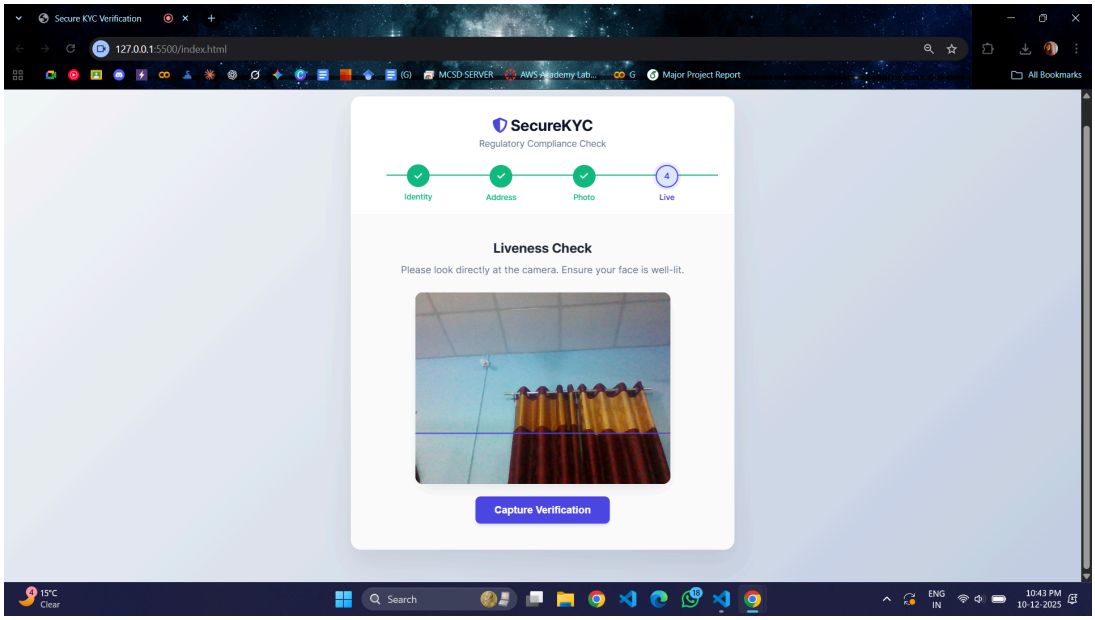

Figure 11: Liveness Check

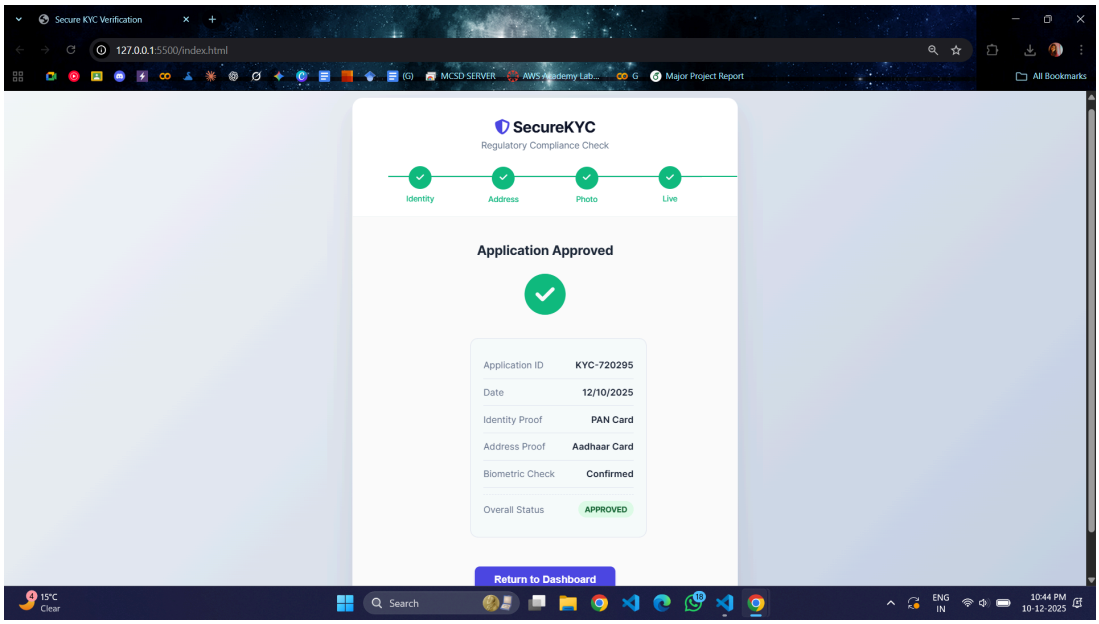

Figure 12: KYC Approved

CONCLUSION

The Optimized Hybrid KYC Verification System addresses critical onboarding inefficiencies by integrating on-device AI with robust server-side processing. This approach targets key failure points, aiming to reduce overall rejections by 50-70% and cut Turnaround Time (TAT) to under 20 seconds. By balancing strict regulatory compliance with a frictionless user experience, the solution minimizes customer abandonment and operational costs. A phased rollout with strategic fallbacks ensures feasibility, ultimately transforming the KYC process from a bottleneck into a competitive advantage for customer acquisition.